Litigation in the Era of Blurred Lines Between Work and Personal Data and Devices

Kelly Woodruff – Partner, Farella Braun + Martel LLP
Racheal Turner – Partner, Farella Braun + Martel LLP
Chrysty Esperanza – Counsel, Square Inc.

ACC Spring Training – March 5, 2015

Case Law — Tab

881 F.Supp.2d 1132
(Cite as: 881 F.Supp.2d 1132)

United States District Court,
N.D. California,
San Jose Division.
APPLE INC., Plaintiff,
v.
SAMSUNG ELECTRONICS CO., LTD., a Korean corporation; Samsung Electronics America, Inc., a New York corporation; and Samsung Telecommunications America, LLC, a Delaware limited liability company, Defendants.

Case No. C 11–1846 LHK (PSG).
July 25, 2012.

Background: Plaintiff in patent infringement suit moved for adverse inference jury instruction against defendant based on its alleged spoliation of evidence.

Holdings: The District Court, Paul S. Grewal, United States Magistrate Judge, held that:
(1) defendant's obligation to preserve evidence was triggered when it received informal notice of patent infringement claims, rather than upon filing of suit;
(2) defendant acted with culpable state of mind in failing to preserve internal company emails;
(3) relevant documents were destroyed; and
(4) spoliation inference instruction to jury was appropriate sanction.

Motion granted in part.

West Headnotes

[1] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

District court has inherent discretionary power to make appropriate evidentiary rulings in response to destruction or spoliation of relevant evidence, and may impose sanctions for spoliation of evidence under its inherent powers to manage its own affairs.

[2] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

District court's inherent power includes ability to levy appropriate sanctions against party who prejudices its opponent through spoliation of evidence that spoliating party had reason to know was relevant to litigation.

[3] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply

170Ak1636 Failure to Comply; Sanctions

170Ak1636.1 k. In general. Most Cited Cases

District court's discretion regarding the form of a spoliation sanction is broad, and can range from minor sanctions, such as awarding attorney fees, to more serious sanctions, such as dismissal of claims, or instructing jury that it may draw an adverse inference.

[4] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

Any remedy applied to a spoliator of evidence should be designed to: (1) deter parties from engaging in spoliation; (2) place the risk of an erroneous judgment on party who wrongfully created the risk; and (3) restore prejudiced party to same position he would have been absent the wrongful destruction of evidence by opposing party.

[5] Federal Civil Procedure 170A 2757

170A Federal Civil Procedure
170AXX Sanctions
170AXX(A) In General
170Ak2756 Authority to Impose
170Ak2757 k. Inherent authority. Most Cited Cases

Sanctions under court's inherent powers must be exercised with restraint and should be appropriate to the conduct that triggered the sanction.

[6] Federal Courts 170B 3610(1)

170B Federal Courts
170BXVII Courts of Appeals
170BXVII(K) Scope and Extent of Review
170BXVII(K)2 Standard of Review
170Bk3576 Procedural Matters
170Bk3610 Sanctions
170Bk3610(1) k. In general. Most Cited Cases
(Formerly 170Bk813)

A court's choice of sanctions is reviewed for an abuse of discretion.

[7] Federal Civil Procedure 170A 1551

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)1 In General
170Ak1551 k. In general. Most Cited Cases

A future litigant is not required to make a request to adverse party to preserve evidence for a possible trial, and a failure to do so does not vitiate the independent obligation of adverse party to preserve such information if adverse party knows or should know of impending litigation.

[8] Federal Civil Procedure 170A 1551

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)1 In General

170Ak1551 k. In general. Most Cited Cases

Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

To avoid sanctions for spoliation of evidence, when a company or organization has a document retention policy, it is obligated to suspend that policy and implement a litigation hold to ensure preservation of relevant documents after the preservation duty has been triggered.

[9] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

Federal Civil Procedure 170A 2173

170A Federal Civil Procedure
170AXV Trial
170AXV(G) Instructions
170Ak2173 k. Necessity and subject matter. Most Cited Cases

Party seeking an adverse inference instruction or other sanctions based on spoliation of evidence must establish: (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a culpable state of mind; and (3) that the evidence was relevant to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense.

[10] Patents 291 1760(1)

291 Patents
291VII Patent Infringement
291VII(C) Actions
291VII(C)1 In General
291k1750 Discovery
291k1760 Production of Documents and Things
291k1760(1) k. In general. Most Cited Cases
(Formerly 291k292.3(1))

Obligation to preserve relevant evidence for possible patent infringement suit was triggered when technology company received presentment notice from its competitor that its products were infringing its patents, rather than at later point when patent infringement suit was actually filed, since it was reasonably foreseeable at time of presentment that litigation would occur; competitor provided a comprehensive summary of its specific patent infringement claims against the company, which established more than just a vague hint that company had violated competitor's intellectual property.

[11] Patents 291 1756

291 Patents
291VII Patent Infringement
291VII(C) Actions
291VII(C)1 In General

291k1750 Discovery
291k1756 k. Failure to respond; sanctions in general. Most Cited Cases
(Formerly 291k292.4)

Defendant in patent infringement suit acted with a conscious disregard of its obligations to preserve relevant evidence for trial, as required for court to find it had engaged in spoliation of evidence, when despite having notice of pending patent infringement litigation it continued to use feature on internal email system which automatically deleted employee email messages after 14 days, and instead relied on employees to manually move relevant documents to their computer hard drive for preservation, but failed to send litigation hold notices to all affected employees to alert them of this process or follow up with employees to ensure compliance with litigation hold.

[12] Patents 291 1756

291 Patents
291VII Patent Infringement
291VII(C) Actions
291VII(C)1 In General
291k1750 Discovery
291k1756 k. Failure to respond; sanctions in general. Most Cited Cases
(Formerly 291k292.4)

Even though it was impossible to determine exact number or full extent of emails destroyed when defendant in patent infringement suit failed to properly put in place litigation hold, but instead continued to use feature on internal email system which automatically deleted employee email messages after 14 days, it was clear that relevant documents had been destroyed, as required for court to find defendant had engaged in spoliation of evidence; key employees involved in development of products at issue had produced either few or no emails, while other individuals who had not utilized 14-day deletion technology had produced thousands.

[13] Patents 291 1756

291 Patents
291VII Patent Infringement
291VII(C) Actions
291VII(C)1 In General
291k1750 Discovery
291k1756 k. Failure to respond; sanctions in general. Most Cited Cases
(Formerly 291k292.4)

Spoliation inference instruction would be given to jury, allowing jury to draw inference that relevant emails destroyed by defendant in patent infringement suit would have been unfavorable, where despite having notice of pending litigation defendant had continued to use feature on internal email system which automatically deleted employee email messages after 14 days, and instead relied on employees to manually move relevant documents to their computer hard drive for preservation, but failed to send litigation hold notices to all affected employees to alert them of this process or follow up with employees to ensure compliance with litigation hold, resulting in destruction of relevant emails from key employees.

***1134** Michael A. Jacobs, Harold J. McElhinny, Jason R. Bartlett, Jennifer Lee Taylor, Morrison & Foerster LLP, San Francisco, CA, for Plaintiff.

ORDER GRANTING–IN–PART APPLE'S MOTION FOR AN ADVERSE INFERENCE JURY INSTRUCTION

PAUL S. GREWAL, United States Magistrate Judge.

In this patent infringement suit, Plaintiff Apple Inc. (“Apple”) seeks an adverse inference jury instruction against Defendants Samsung Electronics Co., LTD. (“SEC”), Samsung Electronics America, Inc. (“SEA”), and Samsung Telecommunications America, LLC (“STA”) (collectively “Samsung”).[FN1]

Samsung opposes.[FN2] At issue is whether Samsung took adequate steps to avoid spoliation after it should have reasonably anticipated this lawsuit and elected not to disable the "auto-delete" function of its home-grown "mySingle" email system.[FN3]

FN1. *See generally* Docket No. 895 (Apple's Mot. for Adverse Inference Jury Instruction).

FN2. *See generally* Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction).

FN3. Only SEC's document preservation policies are at issue here because Samsung affiliates SEA and STA use Microsoft Outlook. *See* Docket No. 895 (Apple's Mot. for Adverse Inference Jury Instruction) at 2 (citing Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction, Ex. 10).

Because the answer to this question is no, the court GRANTS–IN–PART Apple's motion for an adverse inference jury instruction.[FN4]

FN4. In light of the compelling public interest in these issues, the court finds insufficient cause to seal any portions of this opinion or the documents it addresses.

I. INTRODUCTION

Samsung's auto-delete email function is no stranger to the federal courts. Over seven years ago, in *Mosaid v. Samsung*, the District of New Jersey addressed the "rolling basis" by which Samsung email was deleted or otherwise rendered inaccessible.[FN5] *Mosaid* also addressed Samsung's decision not to flip an "off-switch" even after litigation began.[FN6] After concluding that Samsung's practices resulted in the destruction of relevant emails, and that "common sense dictates that [Samsung] was more likely to have been threatened by that evidence," [FN7] *Mosaid* affirmed the imposition of both an adverse inference and monetary sanctions.[FN8]

FN5. 348 F.Supp.2d 332, 333, 339 (D.N.J.2004) (sanctioning Samsung with an adverse inference jury instruction for spoliation and finding that "[p]arties who fail to comply with that obligation [to preserve potentially relevant digital information] do so at the risk of spoliation sanctions").

FN6. *See id.* at 333.

FN7. *Id.* at 338.

FN8. *Id.* at 340.

Rather than building itself an off-switch—and using it—in future litigation such as this one, Samsung appears to have adopted the alternative approach of "mend it don't end it." As explained below, however, Samsung's mend, especially during the critical seven months after a reasonable party in the same circumstances would have reasonably foreseen this suit, fell short of what it needed to do.

*1135 II. LEGAL STANDARDS

A. The Court's Inherent Authority to Impose Spoliation Sanctions

[1][2] Courts are vested with inherent powers arising out of " 'the control necessar[y] ... to manage their own affairs so as to achieve the orderly and expeditious disposition of cases.' " [FN9] This inherent power has been recognized in American jurisprudence for almost two centuries as essential to the orderly administration of the judicial process.[FN10] More recently, the Ninth Circuit has explicitly recognized trial courts' "inherent discretionary power to make appropriate evidentiary rulings in response to the destruction or spoliation of relevant evidence," [FN11] and that sanctions for spoliation of evidence may be imposed

under the court's inherent powers to manage its own affairs.[FN12] The court's inherent powers includes the ability to levy appropriate sanctions against a party who prejudices its opponent through the spoliation of evidence that the spoliating party had reason to know was relevant to litigation.[FN13]

FN9. *Unigard Sec. Ins. Co. v. Lakewood Eng'g & Mfg. Corp.*, 982 F.2d 363, 368 (9th Cir.1992) (quoting *Chambers v. NASCO, Inc.*, 501 U.S. 32, 43, 111 S.Ct. 2123, 115 L.Ed.2d 27 (1991)). *Accord Micron Tech., Inc. v. Rambus Inc.*, 645 F.3d 1311, 1326 (Fed.Cir.2011) (applying Third Circuit law); *Leon v. IDX Sys. Corp.*, 464 F.3d 951, 958 (9th Cir.2006) (citing *Fjelstad v. Am. Honda Motor Co.*, 762 F.2d 1334, 1337–38 (9th Cir.1985)); *Thompson v. U.S. Dep't of Hous. & Urban Dev.*, 219 F.R.D. 93, 100 (D.Md.2003) (quoting *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 590 (4th Cir.2001)); *Adkins v. Wolever*, 554 F.3d 650, 652 (6th Cir.2009); *Flury v. Daimler Chrysler Corp.*, 427 F.3d 939, 944 (11th Cir.2005); *In re NTL, Inc. Secs. Litig.*, 244 F.R.D. 179, 191 (S.D.N.Y.2007).

FN10. *See United States v. Hudson*, 11 U.S. (7 Cranch) 32, 33–34, 3 L.Ed. 259 (1812) (finding that "[c]ertain implied powers must necessarily result to our Courts of justice from the nature of their institution ... because they are necessary to the exercise of all others" and they enable courts to "preserve [their] own existence and promote the end and object of [their] creation").

FN11. *Glover v. BIC Corp.*, 6 F.3d 1318, 1329 (9th Cir.1993).

FN12. *See Leon*, 464 F.3d at 958 (9th Cir.2006). Courts also have authority to sanction a party "who fails to obey an order to provide or permit discovery" pursuant to Federal Rule of Civil Procedure 37(b)(2)(A). *Id.* (internal quotation marks omitted). Here, Fed.R.Civ.P. 37(b)(2) is inapplicable because Samsung has not violated a court order. *Accord Shepherd v. Am. Broad. Co., Inc.*, 62 F.3d 1469, 1474 (D.C.Cir.1995) ("When rules alone do not provide courts with sufficient authority to protect their integrity and prevent abuses of the judicial process, the inherent power fills the gap.").

FN13. *See Glover*, 6 F.3d at 1329.

B. The Various Forms Spoliation Sanctions May Take

[3][4][5][6] A trial court's discretion regarding the form of a spoliation sanction is broad, and can range from minor sanctions, such as the awarding of attorneys' fees,[FN14] to more serious sanctions, such as dismissal of claims [FN15]or instructing the jury that it may draw an adverse inference.[FN16] ***1136** The court's discretion is not, however, without its limits. Courts must weigh several factors when deciding which type of sanction to impose on a spoliator. Any remedy applied to a spoliator "should be designed to: (1) deter parties from engaging in spoliation; (2) place the risk of an erroneous judgment on the party who wrongfully created the risk; and (3) restore 'the prejudiced party to the same position he would have been absent the wrongful destruction of evidence by the opposing party.' " [FN17] Sanctions under these "inherent powers must be exercised with restraint" and should be appropriate to the conduct that triggered the sanction.[FN18]

FN14. *See Leon*, 464 F.3d at 961.

FN15. *See id.* at 958.

FN16. *See In re Oracle Corp. Sec. Litig.*, 627 F.3d 376, 386–87 (9th Cir.2010); *see also*

Trigon Ins. Co. v. United States, 204 F.R.D. 277, 284 (E.D.Va.2001) (noting that the spirit of the spoliation inference is captured in "the maxim *omnia presumunter contra spoliatorem*, which means, 'all things are presumed against a despoiler or wrongdoer.' ") (quoting Black's Law Dictionary 1086 (6th ed.1997)). The roots of the spoliation inference can be traced to the case of *Armory v. Delamirie*, 1 stra. 505, 93 Eng. Rep. 664 (K.B.1722), where a "chimney sweep who sued [a] jeweler for return of the jewel he had found and left with the jeweler [ ] was allowed to infer from the fact that the jeweler did not return the jewel that the stone was 'of the finest water.' " *Nation–Wide Check Corp., Inc. v. Forest Hills Dist., Inc.*, 692 F.2d 214, 218 (1st Cir.1982) (Breyer, J.). Because "the judge instructed the jury to 'presume the strongest against him, and make the value of the *best* jewels the measure of their damages,' " the *Nation–Wide* court took the *Armory* decision as "a clear sign that the inference was designed to serve prophylactic and punitive purposes and not simply to reflect relevance." *Id.*

FN17. *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 521, 534 (D.Md.2010) (explaining that most jurisdictions have identified these factors for "sanction-worthy spoliation"). *Accord Surowiec v. Capital Title Agency, Inc.*, 790 F.Supp.2d 997, 1008 (D.Ariz.2011). *See also Trigon Ins. Co.*, 204 F.R.D. at 287 (finding that "[o]nce spoliation has been established, the sanction chosen must achieve deterrence, burden the guilty party with the risk of an incorrect determination and attempt to place the prejudiced party in the evidentiary position it would have been in but for the spoliation.").

FN18. *Chambers v. NASCO, Inc.*, 501 U.S. 32, 44–45, 111 S.Ct. 2123, 115 L.Ed.2d 27 (1991). A choice of sanction is reviewed for an abuse of discretion. *See Micron*, 645 F.3d at 1326.

C. A Litigant's Duty to Preserve Relevant Evidence

[7] The common law imposes the obligation to preserve evidence from the moment that litigation is reasonably anticipated.[FN19] For example, in *Sampson v. City of Cambridge, Md.*,[FN20] the defendant's duty arose no later than the date when plaintiff's counsel, prior to filing the complaint, asked the defendant by letter to preserve relevant evidence.[FN21] However, a future litigant is not required to make such a request, "and a failure to do so does not vitiate the independent obligation of an adverse party to preserve such information" if the adverse party knows or should***1137** know of impending litigation.[FN22]

FN19. *See Silvestri*, 271 F.3d at 591 ("The duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation."); *Goodman v. Praxair Servs., Inc.*, 632 F.Supp.2d 494, 509 (D.Md.2009) (same); *Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec. LLC*, 685 F.Supp.2d 456, 466 (S.D.N.Y.2010) (Scheindlin, J.) (same) (overruled on other grounds); *Leon*, 464 F.3d at 959 (finding that duty to preserve exists when party had "some notice that the documents were potentially relevant to the litigation before they were destroyed" and "because the relevance of ... [destroyed] documents cannot be clearly ascertained because the documents no longer exist, a party 'can hardly assert any presumption of irrelevance as to the destroyed documents' ") (internal citations omitted) (citing *Alexander v. Nat'l Farmers Org.*, 687 F.2d 1173, 1205 (8th Cir.1982)); Paul W. Grimm et al., *Pro-*

portionality in the Post–Hoc Analysis of Pre–Litigation Preservation Decisions, 37 U. BALT. L.REV. 381, 390 n. 38 ("All circuits recognize the duty to preserve information relevant to anticipated or existing litigation.") (internal citations omitted). "[T]his duty arises at the point in time when litigation is reasonably anticipated whether the organization is the initiator or the target of litigation." THE SEDONA CONF. WORKING GROUP ON ELECTRONIC DOCUMENT RETENTION & PRODUCTION, THE SEDONA CONF. COMMENT ON LEGAL HOLDS: THE TRIGGER AND THE PROCESS 1 1 (public cmt. Aug.2007), *available at* https:// thesedona conference. org/ download- pub/ 77 ("LEGAL HOLDS") (last visited July 24, 2012).

FN20. 251 F.R.D. 172 (D.Md.2008).

FN21. *Id.* at 181.

FN22. *Thompson*, 219 F.R.D. at 100. District courts throughout the Ninth Circuit have repeatedly held that where a party should reasonably know that evidence is potentially relevant to anticipated litigation, that party is under the obligation to preserve that evidence. *See, e.g.*, *United States ex rel. Berglund v. Boeing Co.*, 835 F.Supp.2d 1020, 1049 (D.Or.2011); *Surowiec*, 790 F.Supp.2d at 1005; *Morford v. Wal–Mart Stores, Inc.*, Case No. 2:09–CV–02251 RLH (PAL), 2011 WL 635220, at *3 (D.Nev. Feb. 11, 2011); *Carl Zeiss Vision Intern. GmbH v. Signet Armorlite, Inc.*, Case No. 07–CV–0894 DMS (POR), 2010 WL 743792, at *14 (S.D.Cal. Mar. 1, 2010); *Rev 973 LLC v. Mouren–Laurens*, Case No. CV 98–10690 AHM (Ex), 2009 WL 273205, at *1 (C.D.Cal. Feb. 2, 2009); *In re Napster, Inc. Copyright Litig.*, 462 F.Supp.2d 1060, 1067–68 (N.D.Cal.2006); *Performance Chevrolet, Inc. v. Market Scan Info. Sys.*, Case No. CV–04–0244 BLW, 2006 WL 1042359, at *1 (D.Idaho Apr. 18, 2006). *Cf. Micron*, 645 F.3d at 1320; *Silvestri*, 271 F.3d at 590; *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir.1998).

D. The Scope of a Litigant's Preservation Duties

[8] The duty to preserve evidence also "includes an obligation to identify, locate, and maintain, information that is relevant to specific, predictable, and identifiable litigation." [FN23] It is well-established that the duty pertains only to relevant documents.[FN24] Relevant documents include:

FN23. Legal Holds, at 3.

FN24. *See Pension Comm.*, 685 F.Supp.2d at 466.

> [A]ny documents or tangible things (as defined by Rule 34(a)) made by individuals "likely to have discoverable information that the disclosing party may use to support its claims or defenses." The duty also includes documents prepared for those individuals, to the extent those documents can be readily identified (e.g., from the "to" field in e-mails). The duty also extends to information that is relevant to the claims or defenses of any party, or which is "relevant to the subject matter involved in the action." Thus, the duty to preserve extends to those employees likely to have relevant information-the "key players" in the case.[FN25]

FN25. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 220 (S.D.N.Y.2003) (hereinafter "*Zubulake IV*") (footnotes omitted); *see also Broccoli v. Echostar Commc'ns Corp.*, 229 F.R.D. 506, 510 (D.Md.2005) ("The duty to preserve encompasses any documents or tangible items authored or made by individ-

uals likely to have discoverable information that the disclosing party may use to support its claim or defenses."); *Gates Rubber Co. v. Bando Chem. Indus., Ltd.*, 167 F.R.D. 90, 104 (D.Colo.1996) (finding that before imposing sanctions, a court must be satisfied that the missing evidence would have had some relevance to the proceedings); *Davis v. Grant Park Nursing Home, L.P.*, Case No. 1:08–CV–01764 (PLF/JMF), 2010 WL 4642531, at *1 (D.D.C. Nov. 9, 2010) ("Assessing whether sanctions are warranted for loss of otherwise discoverable information is a function of whether a party has been prejudiced by that loss.").

At the same time, it generally is recognized that when a company or organization has a document retention policy, it "is obligated to suspend" that policy and "implement a 'litigation hold' to ensure the preservation of relevant documents" after the preservation duty has been triggered.[FN26]

FN26. *Goodman*, 632 F.Supp.2d at 511 (quoting *Zubulake IV*, 220 F.R.D. at 218); *see also Pension Comm.*, 685 F.Supp.2d at 466 (same); *School–Link Tech., Inc. v. Applied Res., Inc.*, Case No. 05–2088–JWL, 2007 WL 677647, at *3 (D.Kan. Feb. 28, 2007) (same). A litigation hold might be unnecessary under certain circumstances, and reasonableness is still a consideration. *See Haynes v. Dart*, Case No. 08 C 4834, 2010 WL 140387, at *4–5 (N.D.Ill. Jan. 11, 2010) (finding that a broad litigation hold in each case, when there were 800 pending lawsuits, would cause undue burden).

1138 *E. The Court's Test for Spoliation Sanctions

[9] There is not complete agreement about whether spoliation sanctions are appropriate in any given instance, and, more specifically, whether an adverse inference instruction is warranted. The majority of courts use some variation of the three-part test set forth by Judge Scheindlin in *Zubulake IV* for determining whether to grant an adverse inference spoliation instruction.[FN27] That test is as follows: "[a] party seeking an adverse inference instruction (or other sanctions) based on the spoliation of evidence must establish the following three elements: (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a 'culpable state of mind;'[FN28] and (3) that the evidence was 'relevant' to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense."[FN29] After considering these factors, a court must then consider all available sanctions and determine the appropriate one.[FN30]

FN27. *See Gates*, 167 F.R.D. at 102 (finding that while "the criteria for sanctions cannot be reduced to a formula or standardized test," two factors in particular have taken on significant importance in cases analyzing the necessity of spoliation sanctions: "the culpability of the offender, or the alleged mental state which gave rise to the destruction of evidence, and ... the degree of prejudice or harm which resulted from the actions of the offender").

FN28. Apple makes much of the so-called "Korean Fair Trade Commission ('FTC') Investigation," in which Samsung was fined 400 million won, the largest fine the Korean FTC has ever levied, for spoliation and obstructing an official investigation. *See* Docket No. 895 (Apple's Mot. for Adverse Inference Jury Instruction) at 11–15 (citing Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction, Ex. 1). The court is not persuaded of the weight properly afforded to such evidence, and declines the invitation to include it in its analysis.

FN29. *Zubulake IV*, 220 F.R.D. at 220; *see also Goodman*, 632 F.Supp.2d at 509 (quoting *Thompson*, 219 F.R.D. at 101); *Victor Stanley*, 269 F.R.D. at 520–21. *Accord In re Napster*, 462 F.Supp.2d at 1078.

FN30. *See, e.g.*, *Fujitsu Ltd. v. Federal Express Corp.*, 247 F.3d 423, 436 (2d Cir.2001) ("The determination of an appropriate sanction for spoliation, if any, is confined to the sound discretion of the trial judge and is assessed on a case-by-case basis."); *Wm. T. Thompson Co. v. GNC*, 593 F.Supp. 1443, 1456 (C.D.Cal.1984) ("Imposition of severe sanctions is required in this case by the severity of the abuses that took place.").

III. DISCUSSION

A. Samsung's Preservation Efforts

1. Samsung's "mySingle" Email System

Samsung's default email system is titled "mySingle." [FN31] mySingle was "set up" in 2000.[FN32] The system is proprietary and was created by a Samsung subsidiary named Samsung Data Systems ("SDS").[FN33] mySingle went operational in 2001,[FN34] and is web-based.[FN35] mySingle stores received and sent employee emails on company-wide servers,[FN36] as opposed to dividing the servers ***1139** by business unit,[FN37] and Samsung employees access their mySingle email accounts through a web-based interface.[FN38] mySingle contains a "general guideline [that] calls for all e-mails to be automatically deleted after the passage of two weeks." [FN39] This functionality operates and stores email companywide in Korea, has no exceptions,[FN40] and has been in place since mySingle went operational. [FN41] Samsung uses mySingle in this way because: (1) "it avoids the danger that confidential business information will be misappropriated in the event the computer itself is lost or stolen";[FN42] (2) it is cheaper than using a 30–day retention period;[FN43] (3) it "reduces the amount of information that could inadvertently be disclosed through misdirected ***1140** email, or stolen through unauthorized access or hacking into an employee's email account on the system;" [FN44] and (4) the policy best complies with Korean privacy law.[FN45]

FN31. *See* Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction) at Ex. 10 (3/8/12 Kyu Hyuk Lee 30(b)(6) Dep. Tr., 9:17–20).

FN32. *See id.* at Ex. 10, 11:9–12.

FN33. *See id.* at Ex. 10, 9:23–10:4.

FN34. *See* Docket No. 987 (Decl. of Han–Yeol Ryu in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) ¶ 3 ("SEC has used the mySingle system since 2001.").

FN35. *See id.*

FN36. *See* Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction) at Ex. 10, 13:9–12; *see also id.* at 27:17–28:3 ("Q. How does the mySingle system store the e-mail for the two-week period that exists before the deletion? ... A. It's my understanding that they are stored in the mySingle server."); Docket No. 987 (Decl. of Han–Yeol Ryu in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) ¶ 2 (declaring that mySingle "retains email in a user's inbox and 'sent' folders, for 14 days").

FN37. *See* Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction) at Ex. 10, 13:6–12 ("Q. And is there a server within the Mobile Communications Division where it would be stored? ... A. Well, it's not a server that is

operated by the Mobile Communications Division. It is a group-wide, that is, Samsung group-wide system. So it is within mySingle.").

FN38. *See* Docket No. 987 (Decl. of Han–Yeol Ryu in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) ¶ 3 ("SEC uses an email system known as mySingle to maintain the email accounts of SEC employees, and provide SEC employees with an interface to access their SEC email accounts.").

FN39. *See* Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction) at Ex. 10, 14:1–3; *see also* Docket No. 987 (Decl. of Han–Yeol Ryu in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) ¶ 3 ("Email in a user's inbox and 'sent' folders are retained by the mySingle email system for 14 days.").

FN40. *See* Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction) at Ex. 10, 27:6–15 ("Q. When Samsung found out that Apple was going to bring litigation against it, why didn't Samsung stop the automatic deletion feature of its e-mail system? ... A. mySingle is a system that is used by the entire group at Samsung and there is no separate guidelines that provides any changes to the policy particular [*sic*]."); *see also id.* at 16:4–9 ("Q. And is there any way to automatically have all of the e-mail that comes into a person who works at the Mobile Communications Division go directly onto a hard drive to be saved? A. Well, mySingle does not have that sort of a feature. You'd have to do it separately.").

FN41. *See id.* at 14:7–13 ("Q. Has the policy of deleting e-mails after two weeks at mySingle, has that gone on the last five years? ... A. Well, as for the policies associated with mySingle, ever since the system was first set up they have not changed to date."); *see also* Docket No. 987 (Decl. of HanYeol Ryu in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) ¶ 3 ("SEC has had the 14–day email retention policy in place since 2001.").

FN42. Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) at 6; *see also* Docket No. 987 (Decl. of Han–Yeol Ryu in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) ¶ 4.

FN43. *See* Docket No. 987 (Decl. of Han–Yeol Ryu in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) ¶ 10. Samsung claims that extending the retention policy for its employees would cost an additional $35,983,193 per year. Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) at 6. Even if this claim were beyond mere challenge, Samsung did not estimate the cost of temporarily moving key custodians' email accounts to unique servers that do not biweekly destroy emails, or the cost of temporarily moving key custodians from mySingle to Microsoft Outlook. *See* Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) at 6.

FN44. Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) at 6. *See also* Docket No. 987

(Decl. of Han–Yeol Ryu in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) ¶ 11.

FN45. *See* Docket No. 987 (Decl. of Han–Yeol Ryu in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) ¶ 9.

Employees using mySingle can save any emails they deem relevant.[FN46] The mySingle interface has a "Save All" button that employees can "click" to save all email in their inbox and sent folders to their computer's hard drive. [FN47] If an employee clicks this button every two weeks, all of that employee's emails will be saved.[FN48] Employees also have the option of selecting individual emails or groups of emails, rather than all emails, and saving just these specific emails to their hard drives.[FN49] ***1141** Samsung gives its employees the option of using Microsoft Outlook. [FN50] Microsoft Outlook, unlike mySingle, allows employees to automatically view and archive emails they receive on their local hard drives. [FN51] mySingle's 14–day destruction policy does not apply to locally saved emails on Microsoft Outlook.[FN52] Samsung employees do not require permission to use Outlook for storing email, but they do need its permission to use Outlook for sending email.[FN53]

FN46. *See* Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction) at Ex. 10, 14:3–6 ("However, for those individuals to whom document retention notice is served, they are requested to separately save on their respective hard drives the relevant emails.").

FN47. Samsung's 30(b)(6) witness testified that employees must save each email to their hard drives individually. Samsung now claims for the first time in conjunction with this motion that this testimony was incorrect. *Compare* Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) at 6; Docket No. 987 (Decl. of Han–Yeol Ryu in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) ¶ 5 ("The mySingle interface allows for SEC employees to save all email in their inbox, as well as in their 'sent' folders, to the local hard drive on his or her desktop or laptop computer, by clicking a "Save All" button. An SEC employee who uses this 'Save All' button every two weeks could save all of his or her email to his or her local hard drive."), *with* Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction) at Ex. 10, 16:4–15, 21:6–13 ("Q. And is there a way to automatically have all of the e-mail that comes into a person who works at the Mobile Communications Division go directly onto a hard drive to be saved? A. ***Well, mySingle does not have that sort of feature. You'd have to do it separately.*** Q. So under mySingle system you would have to move each e-mail over from mySingle system into the hard drive in order to preserve it; is that right? ... A. Yes, that is right as far as mySingle system is concerned.... Q. So you [Samsung's 30(b)(6) witness's personal practice] don't click as a group, you click each one and move it separately into the directory, true? A. I suppose everybody does things a little differently from one another, but in my case what I do is click everything all together and then de-click as to spam mails, personal types of e-mails and then move the rest.") (emphasis added).

FN48. Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) at 6. *See also* Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction)

at Ex. 10, 15:20–16:2 ("Q. If I were to-if I worked at the Mobile Communications Division and I want to save my e-mail, would I have to move it over to the hard drive within two weeks in order to preserve it? ... A. Yes, you would copy it to your hard disk drive before its deletion.").

FN49. *See* Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) at 6; *see also* Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction) at Ex. 10, 15:4–18 ("Q. Let's assume a person wants to retain their e-email and doesn't want it to be lost after two weeks, and they work at the Mobile Communications Division. What do they have to do to retain their e-mail? A. Well, it's actually the same case for both the Mobile Communications Division as well as other units in that for those who desire to save any of their own emails they can separately park those in their hard drives. Q. How do they do that? A. Well, whatever e-mail they desire to move, they can move that over to a directory in their hard drive.").

FN50. *See* Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) at 6–7; Docket No. 987 (Decl. of Han–Yeol Ryu in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) ¶ 7.

FN51. *See id.*

FN52. *See* Docket No. 987 (Decl. of Han–Yeol Ryu in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) ¶ 8.

FN53. *See* Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) at 7 n. 8; *see also* Docket No. 987 (Decl. of Han–Yeol Ryu in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) ¶ 5. Samsung's 30(b)(6) deponent previously stated, however, that employees need their supervisor's permission to use Microsoft Outlook. *See* Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction) at Ex. 9, 164:19–165:7. ("Q. In order for an employee to store e-mail to avoid having the email automatically deleted after two weeks, the employee has to obtain permission from the head of his or her department to use the Outlook system; is that correct? ... A. In order to install an Outlook linked to mySingle, you have to get permission, but even though you don't use the Outlook system, you can separately store that kind of information on your personal hardware drive.") Samsung now claims that SEC requires employees only to "obtain special permission to use Outlook to *send* email, but there is no such requirement for employees to use Outlook to view and archive email." Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) at 7 n. 8 (citing Decl. of Han–Yeol Ryu in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction ¶ 7).

It is within each Samsung employee's discretion whether to save relevant documents.[FN54] Samsung has never attempted to verify whether Samsung employees are complying with the instructions they were told to follow. [FN55] mySingle does have a feature, however, that reminds employees ***1142** when the time for biweekly deletion of their emails is near.[FN56] "The 'Help' page in mySingle explains in both English and Korean how to use the 'Save All' function," [FN57] as well as "how to save individual emails or groups of emails." [FN58]

FN54. *See* Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction) at Ex. 10, 18:11–24 ("Q. So Samsung relied on each individual person to move each of their e-mails that would be related to the litigation from mySingle system onto the hard drives of their individual computers; is that true? ... A. Again, with respect to document retention requests, the overall need for such and the importance, indeed, as well as the methodology for such are explained to our people on numerous occasions by way of the notice as well as explanations and then put into practice. And it is my understanding that those persons who have been so notified have faithfully abided by said duty.").

FN55. *See* Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction) at Ex. 10, 19:1–15, 32:9–33:25 ("Q. So after the preservation notice is given out, Samsung does not check to make sure that the employees who receive the document retention notice are actually moving e-mails within the two-week period before their automatic deletion, true? ... A. First of all, such document preservation requests will be given to thousands of employees; however, there is no way to check on to see one by one whether document deletion is actually happening. However, since there would be sufficient explanation given for the importance and methodology that the recipient of the notice should go by, I believe that these documents are preserved accordingly.... Q. So, Mr. Lee, Samsung does not check to make sure the employees are following directions in the document retention notice, right? ... A. Since on numerous occasions that IP legal team attorneys and outside attorneys provide numerous explanations about the notice and also regarding the notice's importance, necessity and methodology of preservation, on that basis I understand that the persons who are required to preserve those documents would precisely save those documents. Q. So you trust those people to follow the document retention notice and you don't follow up and check with them to make sure they do so? ... A. Since there would have been sufficient notification as to the importance and methodologies concerning preservation of documents, one would have a conviction that such relevant document be well-preserved accordingly. ***However, there is no way to check on to see if such documents are discarded.*** Q. Well, you would agree with me that one way to make sure that such emails are not deleted would be to back up the e-mail system on a regular basis so that it does not get deleted after two weeks, right?") (emphasis added).

FN56. *See id.* at 26:3–11 ("Q. How do they know about it [the deletion]? ... A. There's a certain indication with respect to each and every piece of mail that it's so many days before deletion. Q. And is that true for every employee at Samsung? A. Yes, the system makes that indication.").

FN57. Docket No. 987 (Decl. of Han–Yeol Ryu in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) ¶ 5.

FN58. *Id.* ¶ 6.

2. Samsung's Issuance of Litigation Hold Notices

On August 4, 2010, Apple presented Samsung with information regarding Samsung's infringement of certain Apple patents.[FN59] Soon after, in an email dated

August 23, 2010, Samsung emailed litigation hold notices to certain Samsung employees.[FN60] The notice reads, in relevant part: **"[T]here is a reasonable likelihood of future patent litigation between Samsung and Apple unless a business resolution can be reached."** [FN61] The email then goes on:

> FN59. *See* Docket No. 895 (Apple's Mot. for Adverse Inference Jury Instruction) at 2. According to Apple, it began negotiations with Samsung regarding Samsung's "copying of Apple's design ... in July 2010, when Samsung launched its Galaxy line of smartphones bearing a striking resemblance to Apple's own iPhone products. That month, Apple's CEO Steve Jobs and Apple's Chief Operating Officer Tim Cook met with Samsung CEO J.Y. Lee. Both Mr. Jobs and Mr. Cook advised Mr. Lee that Samsung needed to cease copying Apple's iPhone designs and infringing Apple's patents immediately. On August 4, 2010, Apple's General Counsel Bruce Sewell and I met with Dr. Seungho Ahn, Samsung Electronics' Vice President and Head of its Intellectual Property Center, in Cupertino. During our meeting, I gave a presentation illustrating Samsung's infringement of Apple's patents. I also emphasized that Samsung had other design options that would take its products farther away from Apple's products and avoid direct conflict." Docket No. 128 (Decl. of Richard J. Lutton, Jr. in Supp. of Apple's Mot. for a Prelim. Inj.) ¶¶ 2–4.
>
> FN60. *See* Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction) at Ex. 9. Samsung also sent the same notice again on September 3, 2010. In total, 27 Samsung custodians received either the August 23 or September 3, 2010 litigation hold notice. *See id.* In contrast, the litigation hold notices sent on April 21, 2011, and those sent after, were addressed to 2,841 custodians. *See id.*
>
> FN61. *Id.* (emphasis added). The qualifier, "unless a business resolution can be reached," is of course true of virtually all litigation amongst commercial competitors, and for that reason is not at all determinative.

The key issue that courts consider in determining whether or not a duty to preserve exists centers on whether the party had notice of the relevance of the evidence in question to anticipated litigation. The notice can arise from many different things, including prior lawsuits, prelitigation communications, or any preparatory steps and efforts undertaken for the anticipated litigation.[FN62]

> FN62. *Id.*

The notice requests that employees "preserve any and all such documents that may ***1143** be relevant to the issues in a potential litigation between Samsung and Apple until it is fully resolved." [FN63] The notice lists ten discreet categories of documents that Samsung employees receiving the email "should nevertheless retain and preserve."[FN64] No significant further action was taken over the next seven months.

> FN63. *Id.*
>
> FN64. Samsung's August 23, 2010 litigation hold notice contains 10 discreet categories of documents to be preserved, while Samsung's April 21, 2011 litigation hold notice contains 15 discreet categories of documents. While the April 21, 2011 notice is certainly more comprehensive, there is substantial overlap between the two notices. *See* Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction) at Ex. 9A and 9C. This weighs heavily

against Samsung's argument that it could not have known in late-August 2010 what might be relevant to litigation with Apple. *See* Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) at 15 n. 16 ("Apple seeks to penalize Samsung for its voluntary decision to send out a limited litigation hold notice to certain employees when it began general licensing discussions with Apple in 2010, turning Samsung's positive efforts—not followed by Apple itself—against it. The law makes clear that the duty to preserve at issue here was not triggered until Apple filed its precise claims."). Samsung cites to a single decision for this proposition, namely, *FTC v. Lights of America, Inc., et al.*, Case No. SACV 10–1333 JVS (MLGx), 2012 WL 695008 (C.D.Cal. Jan. 20, 2012) (hereinafter " *LOA* "). but *LOA* is distinguishable. *LOA* dealt with the unique situation in which a government agency is required to issue a litigation hold. *LOA* held that the FTC was not obligated *per se* to issue a litigation hold "at the commencement of the full-phase investigation or upon the issuance of the CID because litigation was not 'reasonably foreseeable' at those points." *Id.* at *3. *LOA* also noted that FTC investigations are designed for gathering information, and many investigations end without litigation. *See id.*

On April 15, 2011, Apple filed this lawsuit. On April 21, 2011, Samsung again sent litigation hold notices, this time to 2,300 Samsung employees, detailing the scope of the documents subject to preservation.[FN65] Over the next few weeks, Samsung sent additional amended litigation hold notices to over 2,700 Samsung employees.[FN66] Samsung continued to update both the population of employees receiving notices, as well as the content of the notices, as the litigation between Apple and Samsung took shape.[FN67] The litigation hold notices included the following language: "if you have any doubt as to whether you should preserve particular documents, you are instructed to retain them. Please distribute ***1144** this message to anyone who may have such relevant documents." [FN68] The notice goes on to admonish employees, in bolded capital letters, not to destroy any responsive documents, but to instead preserve them.[FN69] Between May 2 and May 4, 2011, Samsung's outside counsel sent several members of its firm to Korea to assist Samsung's in-house counsel with educating Samsung employees on their duty to preserve relevant documents and Samsung's collection efforts.[FN70]

FN65. *See* Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) at 7–8 (citing Decl. of Thomas R. Watson in Supp. of Opp'n to Apple's Mot. for Adverse Inference Jury Instruction, Ex. 1).

FN66. *See id.* at 8 (citing Decl. of Thomas R. Watson in Supp. of Opp'n to Apple's Mot. for Adverse Inference Jury Instruction, Ex. 1).

FN67. *See* Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Instruction) at 7–9; *see also* Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction) at Ex. 10, 31:8–32:8 ("Q. What has Samsung done to make sure that the thousands of employees who received the document retention notice are actually moving their e-mails on their personal computers from the mySingle system onto a separate directory within the two-week period that that [*sic*] must occur to prevent the deletion of their e-emails? ... A. At the time the document preservation notice is given by the IP legal team or outside counsel, upon receipt of such notice by the officers and employees of Samsung, they are fully apprised of the importance. The neces-

sity and methodology that they should go by in preserving such documents pursuant to the notice. And since IP legal team members sufficiently provide explanations as to development departmental leaders, the recipients conduct good-faith compliance of such notice and therefore it will be difficult to check on to see whether there would be a non-preservation of such notice after the request is given out.").

FN68. Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) at 8 (citing Decl. of Thomas R. Watson in Supp. of Opp'n to Apple's Mot. for Adverse Inference Jury Instruction, Ex. 33 at Ex. A).

FN69. *Id.*

FN70. *See id.* at 9 n. 10 (citing Decl. of H. Kang in Supp. of Opp'n to Apple's Mot. for Adverse Inference Jury Instruction ¶ 12; Decl. of Sara Jenkins in Supp. of Opp'n to Apple's Mot. for Adverse Inference Jury Instruction ¶ 10).

3. Samsung's Efforts to Follow-up with its Relevant Employees

After sending litigation hold notes to its employees, Samsung explained to its relevant department heads the specifics of Samsung's litigation hold efforts. [FN71] Samsung's in-house IP legal team, as well as Samsung's outside counsel, all were involved in these efforts.[FN72] Samsung's in-house document preservation team provided relevant Samsung employees with numerous explanations on numerous occasions about the litigation hold notice, its importance, and the necessity and methodology of document preservation. [FN73] More specifically, at the end of April 2011, Samsung's IP Legal Team Director held four follow-up meetings with over 300 Samsung employees. [FN74] The purpose of these meetings was to educate key employees about the United States' litigation discovery system, and the requirements of Samsung's computer system for document preservation.[FN75] Samsung also imparted to its employees the importance of actively saving emails and other electronic documents, and exactly how to do so.[FN76] Samsung employees were also told to contact the IP Legal Team if they had additional questions. [FN77] All Samsung employees attending these meetings were instructed to pass what they had learned on to their "junior managers."[FN78]

FN71. *See id.* (citing Decl. of Thomas R. Watson in Supp. of Opp'n to Apple's Mot. for Adverse Inference Jury Instruction, Ex. 5 (3/8/12 Kyu Hyuk Lee 30(b)(6) Dep. Tr., 19:6–13)).

FN72. *See id.*

FN73. *See id.*

FN74. *See id.*

FN75. *See id.*

FN76. *See id.* at 8–9.

FN77. *See id.* at 9.

FN78. *See id.*

B. Application of the Court's Spoliation Test

1. Samsung's Duty to Preserve Relevant Evidence

[10] Apple argues that Samsung's discovery obligation arose in August 2010 based on the August 4, 2010 presentation Apple gave to Samsung regarding Apple's contention that certain Samsung products infringe certain Apple patents.[FN79] Apple goes on to argue that Samsung must have known in August 2010 that it had no plans to alter its products, and thus a

reasonable party in Samsung's place would have known that litigation with Apple was imminent, if not inevitable.[FN80]

FN79. *See* Docket No. 1047 (Apple's Reply in Supp. of Mot. for Adverse Inference Jury Instruction) at 2–3.

FN80. Apple notes that Samsung made it clear to Apple in Spring 2011 that Samsung would not seek a negotiated end to their disagreements. According to Apple, Samsung announced the release of "a new round of infringing products" in Spring 2011. *See* Docket No. 1047 (Apple's Reply in Supp. of Mot. for Adverse Inference Jury Instruction) at 2–3.

***1145** Samsung responds that its preservation obligations arose on April 15, 2011, when Apple filed its complaint in this matter. According to Samsung, mySingle and its 14–day destruction policy were adopted for legitimate business purposes, Samsung could not have known in August 2010 which claims Apple might assert against it, and a negotiated settlement with Apple was still possible in August 2010 because licensing discussions with Apple were ongoing.

The court agrees with Apple. The phrase "reasonably foreseeable" as it relates to a party's preservation duties sets an objective standard.[FN81] On August 4, 2010, Apple presented Samsung with more than just a vague hint that it believed Samsung had violated its intellectual property. Apple delivered, in person, a comprehensive summary of its specific patent infringement claims against specific Samsung products. Whatever hopes Samsung might have subjectively held for a license or other non-suit resolution, this would certainly put a reasonably prudent actor on notice that litigation was at least foreseeable, if not "on the horizon." [FN82] If there were any doubts about this, Samsung itself resolved them. Shortly after Apple's presentation Samsung sent litigation hold notices to a small number of Samsung employees that read, in relevant part: ***"there is a reasonable likelihood of future patent litigation between Samsung and Apple unless a business resolution can be reached."*** [FN83] And yet other than exhorting these employees to circumvent the otherwise certain destruction of relevant materials, for seven months Samsung did no follow-up training at all. And at no time, even up to the present day, did Samsung engage in any audit of these employees to gauge what effect, if any, its exhortations were having.

FN81. *See Micron,* 645 F.3d at 1320 (" '[S]poliation refers to the destruction or material alteration of evidence or to the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation.' This is an objective standard, asking not whether the party in fact reasonably foresaw litigation, but whether a reasonable party in the same factual circumstances would have reasonably foreseen litigation. When litigation is 'reasonably foreseeable' is a flexible fact-specific standard that allows a district court to exercise the discretion necessary to confront the myriad factual situations inherent in the spoliation inquiry.") (internal citations omitted).

FN82. Samsung's argument that Apple failed to issue litigation hold notices in August 2010 is irrelevant to the court's determination here. Samsung has always been free to argue, at the appropriate time, that Apple too is guilty of spoliation. In any event, that motion is not currently before the court.

FN83. Docket No. 1047 (Apple's Reply in Supp. of Mot. for Adverse Inference Jury Instruction) at 2; *see also* Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's

Mot. for Adverse Inference Jury Instruction) at Ex. 9.

Samsung cannot on the one hand tout its prudence and responsibility in regards to its post-complaint preservation efforts, and simultaneously argue that it was ignorant of the possibility of litigation pre-complaint. This is not a matter of "punishing" a party for taking prudent steps to avoid controversy. It is a matter of holding a party to what could not be a plainer admission. In sum, the court finds that Samsung's duty to preserve evidence arose on August 23, 2010, the date Samsung issued litigation hold notices to its employees following Apple's infringement presentation to Samsung.[FN84]

FN84. Samsung euphemistically refers to Apple's infringement presentation as a "licensing discussion." *See* Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) at 15 n. 16.

***1146** *2. Samsung's Requisite Mental State*

Even as litigation with Apple was "reasonably foreseeable," Samsung kept its auto-delete policy in place at all times. Apple argues that Samsung's actions evidence the necessary "culpable state of mind."[FN85] According to Apple, Samsung's later efforts to educate its employees, and its issuance of litigation hold notices, do not negate this.[FN86] It is Samsung's continued use of its biweekly email destruction policy, Apple argues, without any methodology for verifying whether Samsung employees at all complied with the instructions they were given, that is dispositive to the instant question. [FN87] In other words, it is Samsung's failure to monitor its employees' efforts downstream, as opposed to its immediate efforts to educate its employees after Apple filed this lawsuit, which violates Samsung's duty to preserve relevant documents.

FN85. *See Leon,* 464 F.3d at 959 (internal citations omitted) ("A party's destruction of evidence qualifies as willful spoliation if the party has some notice that the documents were *potentially* relevant to the litigation before they were destroyed."); *see also Unigard,* 982 F.2d 363, 368 n. 2 (9th Cir.1992) ("This court has, since *Roadway* [*Express, Inc. v. Piper,* 447 U.S. 752, 100 S.Ct. 2455, 65 L.Ed.2d 488 (1980)], confirmed the power of the district court to sanction under its inherent powers not only for bad faith, but also for willfulness or fault by the offending party.") (citing *Halaco Eng'g Co. v. Costle,* 843 F.2d 376, 380 (9th Cir.1988)); *Glover,* 6 F.3d at 1329 ("As *Unigard* correctly notes, however, a finding of 'bad faith' is not a prerequisite to this corrective procedure. Surely a finding of bad faith will suffice, but so will simple notice of 'potential relevance to the litigation.' ") (internal citations omitted) (citing *Akiona v. United States,* 938 F.2d 158, 160–61 (9th Cir.1991)).

FN86. *See* Docket No. 895 (Apple's Mot. for Adverse Inference Jury Instruction) at 3–4. Apple makes the additional argument that Samsung's August 23, 2010 litigation hold notice was deficient because it failed to instruct employees regarding how precisely to preserve emails, and failed to even mention mySingle's automatic deletion feature. *See id.* at 4 (citing Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction, Ex. 9 at A, C, E, G (English versions), I–J). The court agrees. Samsung's August 23, 2010 notice fails to specifically instruct its recipients how to preserve relevant evidence, instead stating only, "[t]to the extend the need to retrieve copies of potentially relevant documents arises, representatives of Samsung's IP Legal Team will be contacting you. In the meantime, if you have any questions, please call the Personnel of the IP Legal Team." *Id.* Considering that

> Samsung claims its biweekly email destruction policy has no exceptions and cannot be shut down absent prohibitive cost, the court wonders how a custodian can "immediately suspend[ ]" a "scheduled disposal." In any event, the court would have reached the same decision regardless of whether Samsung's August 23, 2010 notice included detailed preservation instructions because the notice was sent to only a comparatively small number of Samsung employees, and Samsung never followed-up to check if its employees were at all in compliance with these instructions.
>
> FN87. *See id.* at 4.

Samsung responds that Apple has not met its burden of showing that the spoliation was "intentional" or "willful," and that Apple's complaint that Samsung might have "done more" to preserve relevant evidence is "insufficient as a matter of law to establish 'bad faith' " in the Ninth Circuit.[FN88]

> FN88. Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) at 19–22 (citing *Glover*, 6 F.3d at 1329 (9th Cir.1993) ("A party should only be penalized for destroying documents if it was wrong to do so, and that requires, at a minimum, some notice that the documents are potentially relevant."); *Akiona*, 938 F.2d at 161 (reversing adverse inference ruling where plaintiffs failed to show "any bad faith in the destruction of the records, nor even that the government was on notice that the records had potential relevance to the litigation" and noting no intent to cover up information)).

***1147** [11] The court agrees with Apple. Samsung may be right that the record does not establish any bad faith on its part. But bad faith is not the required mental state for the relief Apple seeks. All that the court must find is that Samsung acted with a "conscious disregard" of its obligations.[FN89] In light of its biweekly automatic destruction policy, Samsung had a duty to verify whether its employees were actually complying with the detailed instructions Samsung claims it communicated to them.[FN90] As far as the court can see, Samsung did nothing in this regard.[FN91] Samsung failed to send litigation hold notices in August 2010, beyond a select handful of employees, when its duty to preserve relevant evidence arose. Samsung provided no follow-up, and instead waited to send such notices and to follow-up with individual employees for seven more months, after Apple filed its complaint. And again, at all times, Samsung never checked whether even a single Samsung custodian was at all in compliance with the given directives, while at all times the 14–day destruction policy was in place. This is more than sufficient to show willfulness.

> FN89. *See Hamilton v. Signature Flight Support Corp.*, Case No. 05–0490, 2005 WL 3481423, at *7 (N.D.Cal. Dec. 20, 2005) (finding that whether a party has "consciously disregarded" its preservation duties to be determinative); *see also Io Group, Inc. v. GLBT, Ltd.*, Case No. C–10–1282 MMC (DMR), 2011 WL 4974337, *5 (N.D.Cal. Oct. 19, 2011) ("The court concludes Defendants 'consciously disregarded' their obligation to preserve relevant evidence.") (citing *Hamilton*, 2005 WL 3481423, at *7). The court notes that in resolving a similar motion Apple brought against Samsung before the ITC, the Commission applied the stricter "bad faith" standard. But as the Ninth Circuit has confirmed, while bad faith may be sufficient for sanctions, it is not necessary. *See Unigard*, 982 F.2d at 368 n. 2.
>
> FN90. *See* Docket No. 895 (Apple's Mot. for Adverse Inference Jury Instruction) at 4.

Samsung's 30(b)(6) witness was asked during his deposition "what [relevant Samsung employees] have done to abide by their duty." In response, Samsung's 30(b)(6) witness stated, "Well, the question is a little vague for my purposes, but, again, with respect to document retention requests, we impress upon our people as to how important that is and how it ought to be carried out. And, indeed, our counsel within the IP legal team as well as outside counsel all get involved in this, and notices are sent out, people are brought up to speed as to those aspects and the respective department heads are all sufficiently notified as to this. So it is my understanding that the results thereof are in fact preserved intact." Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction) at Ex. 10, 19:1–15.

FN91. *See, e.g.*, Decl. of Sara Jenkins in Supp. of Opp'n to Apple's Mot. for Adverse Inference Jury Instruction, ¶¶ 5–14 (detailing Samsung's post-complaint efforts to educate its employees regarding their preservation obligations).

3. The Relevance of the Destroyed Evidence to Apple

[12] Apple points to the productions of several key Samsung employees that: (1) used the mySingle email system; (2) during the relevant time period; (3) failed to themselves produce much if any relevant emails; and (4) only after other custodian recipients produced one or more of these emails did Apple discover that Samsung may have destroyed relevant evidence. Apple points out that Samsung has produced no email or only a handful of emails from the custodial files of at least 14 key fact witnesses.[FN92] The productions of the following custodians are particularly noteworthy:

FN92. *See* Docket No. 895 (Apple's Mot. for Adverse Inference Jury Instruction) at 4 (citing Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction ¶ 4).

• Won Pyo Hong, the head of Samsung's Product Strategy Team, which includes the Design Group responsible for designing Samsung's ***1148** "Galaxy" smart phones and tablet computers.[FN93] Dr. Hong received the August 23, 2010 litigation hold notice.[FN94] Dr. Hong did not produce any emails and only 18 documents.[FN95] Dr. Hong failed to preserve his April 17, 2011 email regarding comparisons of Apple products that the court cited in granting Apple's motion to compel his deposition.[FN96] Dr. Hong also failed to preserve an email he received that described how Samsung needed to respond to the iPad2 with a slimmer Galaxy Tab.[FN97]

FN93. *See id.* (citing Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction ¶ 5).

FN94. *See id.* (citing Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction, Ex. 9 at S).

FN95. *See id.* (citing Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction ¶ 5).

FN96. *See id.* (citing Docket No. 850 (Order Granting–In–Part Mot. to Compel) at 9–10).

FN97. *See* Docket No. 895 (Apple's Mot. for Adverse Inference Jury Instruction) at 4–6 (citing Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction ¶ 6 and Ex. 2).

• Minhyouk Lee, the head Samsung designer responsible for the industrial design of Samsung's

accused Galaxy S products, did not produce any emails; [FN98]

FN98. *See id.* at 5 (citing Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction ¶ 7). Other custodians produced 155 emails from Mr. Lee. *See* Decl. of Alex Binder in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction ¶ 19.

• Joon–Il Choi, a senior manager in Samsung's R & D Management Group, did not produce any emails.[FN99] Mr. Choi, however, presided over and wrote notes for a meeting that Gee–Sung Choi, Samsung's former President and CEO of its digital media division and current Vice Chairman of Corporate Strategy, [FN100] attended on March 5, 2011, to discuss alterations to the Galaxy Tab 10.1 to make it more competitive with the newly released thinner iPad 2. [FN101]

FN99. *See id.* (citing Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction ¶ 8). Other custodians produced 112 emails from Mr. Choi. *See* Decl. of Alex Binder in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction ¶ 19.

FN100. *See* SAMSUNG ELEC., Board of Directors, http:// www. samsung. com/ us/ aboutsamsung/ ir/ corporate governance/ boardof directors/ IRGee Sung Choi. html (last visited July 24, 2012).

FN101. *See* Docket No. 895 (Apple's Mot. for Adverse Inference Jury Instruction) at 5 (citing Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction ¶ 9 and Ex. 3).

• Don–Joo Lee, the head of sales and marketing for Samsung's mobile business unit, and who is in charge of promoting and selling Samsung mobile products globally, including the Galaxy S products.[FN102] Mr. Lee produced 16 emails, and failed to preserve emails regarding Samsung's response to the iPad 2, including emails discussing Samsung's need to fight the iPad 2 with a slimmer Galaxy Tab, and the response to Verizon's iPhone and the impact it would have on Samsung.[FN103]

FN102. *See id.* (citing Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction ¶ 22, Ex. 25 at 23:15–23, Ex. 18 at 33:12–13).

FN103. *See id.* (citing Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction ¶¶ 10–12 and Exs. 2, 4, 5). Other custodians produced 420 emails from Mr. Lee. *See* Decl. of Alex Binder in Supp. of Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction ¶ 19.

***1149** • Nara Cho, a senior manager in Samsung's wireless business division, handled product planning for Samsung's tablet devices since early 2010.[FN104] Samsung produced only two emails from Mr. Cho, none of which discuss the Galaxy Tab 10. 1, an accused product that was launched after Apple filed this lawsuit.[FN105]

FN104. *See id.* at 6 (citing Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction ¶ 20 and Ex. 31 at 6:20–10:9, 23:14–21).

FN105. *See id.* (citing Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction ¶ 20).

In contrast, similarly-situated Samsung em-

ployees that use Microsoft Outlook, rather than mySingle, produced many times more. For example, Wookyun Kho produced 7,594 emails, and Junho Park produced 6,005 emails.[FN106]

FN106. *See id.* (citing Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction ¶ 22, Ex. 25 at 23:15–23, Ex. 18 at 33:12–13).

While the nature of the auto-delete function is such that the court will never know how much relevant material was lost, the court cannot ignore the statistical contrast depicted above.[FN107] Samsung acknowledges that "the majority of the accused products at issue here released prior to April 15, 2011," [FN108] meaning the most relevant emails were subject to Samsung's biweekly destruction policy before Samsung undertook the bulk of its preservation efforts. Samsung had ample notice that the evidence was potentially relevant to litigation. Samsung to this day has not suspended its email system's biweekly automatic destruction policy,[FN109] even as to key custodians, nor has it presented any evidence that Samsung employees have at all complied with the instructions they were given. The court must conclude that Samsung "consciously disregarded" its obligation to preserve relevant evidence.[FN110]

FN107. *See Leon*, 464 F.3d at 959 (finding that duty to preserve exists when party had "some notice that the documents were potentially relevant to the litigation before they were destroyed" and "because the relevance of ... [destroyed] documents cannot be clearly ascertained because the documents no longer exist, a party 'can hardly assert any presumption of irrelevance as to the destroyed documents' ") (internal citations omitted).

FN108. *See* Docket No. 987 (Samsung's Opp'n to Apple's Mot. for Adverse Inference Jury Instruction) at 15.

FN109. *See* Docket No. 895 (Decl. of Esther Kim in Supp. of Apple's Mot. for Adverse Inference Jury Instruction) at Ex. 10, 29:8–24 ("Q. But despite this knowledge of its obligations in the United States, Samsung has continued with its policy of deleting e-mails two weeks after their creation using mySingle system, right? ... A. ***Although there has not been any changes to the policy concerning mySingle system,*** in the event necessary there needs any document to be preserved, relevant document preservation requests will be given to personnel who's charged with such request. And the explanation was given by outside and inhouse counsel about the importance and methodology to be used in terms of preservation of those documents. And pursuant to such a request in compliance with the request and the sufficient report was made for the purpose of preservation.") (emphasis added).

FN110. *See Hamilton*, 2005 WL 3481423, at *7 (listing cases issuing sanctions for failure to preserve evidence appropriate "only when a party has consciously disregarded its obligation to do so"); *see also Mosaid v. Samsung*, 348 F.Supp.2d 332, 338 (D.N.J.2004) (ordering an adverse inference jury instruction be given against Samsung for spoliation of relevant evidence, and finding that "Samsung willfully blinded itself, taking the position that Mosaid's document requests did not seek e-mails and therefore Samsung has no obligation to prevent their continued destruction while this litigation continued").

1150** ***C. The Form of the Sanction

[13] Individually, and certainly collectively, these facts support imposition of some form of sanction.

Samsung's failure to issue sufficiently distributed litigation hold notices on August 23, 2010, and Samsung's failure to monitor its custodial employees' preservation efforts in the face of its biweekly destruction policy once litigation holds issued, warrants sanctions. The court is mindful, however, that any sanction must be the least drastic available to adequately mitigate the prejudice Apple suffered.[FN111]

FN111. *See Chambers,* 501 U.S. at 44–45, 111 S.Ct. 2123 (holding that the court's choice of sanction should be appropriate to the conduct that triggered the sanction).

When applying the spoliation inference, courts are faced with a dilemma. By the very nature of the spoliation, there is no way to know what the spoliated evidence would have revealed, and so courts have to instruct the jury that they are allowed to infer a certain fact or set of facts from the absence of specific evidence. With this in mind, courts have formulated adverse inference instructions that range in their level of severity.

Pension Committee addressed just this issue.[FN112] *Pension Committee* begins, "[l]ike many other sanctions, an adverse inference instruction can take many forms, again ranging in degrees of harshness." [FN113] The degree of harshness should be dictated by the "nature of the spoliating party's conduct—the more egregious the conduct, the more harsh the sanction." [FN114] "In its most harsh form, when a spoliating party has acted willfully or in bad faith, the jury can be instructed that certain facts are deemed admitted and must be accepted as true. At the next level, when a spoliating party has acted willfully or recklessly, a court may impose a mandatory presumption."[FN115] At the other end of the spectrum, "the least harsh instruction permits (but does not require) a jury to presume that the lost evidence is both relevant and favorable to the innocent party. If it makes this presumption, the spoliating party's rebuttal evidence must then be considered by the jury, which must then decide whether to draw an adverse inference against the spoliating party." [FN116]

FN112. 685 F.Supp.2d at 470.

FN113. *Id.*

FN114. *Id.*

FN115. *Id.*

FN116. *Id.*

Apple has suffered prejudice as a result of Samsung's spoliation of evidence. Apple has highlighted several key Samsung custodians, noted above, that both used mySingle and produced little or even no relevant documents. In contrast, Samsung custodians using Microsoft Outlook produced literally thousands of documents. Finally, the mySingle custodians Apple points to are senior Samsung employees whose internal communications would have been especially probative to the claims at issue in this litigation.

On this record, the court concludes that Samsung's preservation efforts failed because: (1) Samsung did not to suspend mySingle's automatic biweekly destruction policy; (2) Samsung failed to issue sufficiently distributed litigation hold notices after Samsung itself admitted that litigation was "reasonably foreseeable," and to follow up with the affected employees for seven months as it later showed it knew how to do; and (3) at all times Samsung failed to monitor its employees' preservation efforts to ensure its employees were at all compliant. In effect, Samsung kept the shredder on long after it should have known about this litigation, and simply trusted its custodial employees to save relevant ***1151** evidence from it. The stark difference in production from mySingle and Microsoft Outlook custodians makes clear that this plan fell woefully short of the mark.

The court finally turns to the appropriate language for an adverse inference instruction in this instance. In the absence of any finding of bad faith, and the court's finding that Samsung acted with conscious disregard of its obligations, or willfully, the court orders the jury be instructed as follows:

> Samsung has failed to prevent the destruction of relevant evidence for Apple's use in this litigation. This is known as the "spoliation of evidence."
>
> I instruct you, as a matter of law, that Samsung failed to preserve evidence after its duty to preserve arose. This failure resulted from its failure to perform its discovery obligations.
>
> You also may presume that Apple has met its burden of proving the following two elements by a preponderance of the evidence: *first*, that *relevant* evidence was destroyed after the duty to preserve arose. Evidence is relevant if it would have clarified a fact at issue in the trial and otherwise would naturally have been introduced into evidence; and *second*, the lost evidence was favorable to Apple.
>
> Whether this finding is important to you in reaching a verdict in this case is for you to decide. You may choose to find it determinative, somewhat determinative, or not at all determinative in reaching your verdict.[FN117]

FN117. *See Johnson v. Wells Fargo Home Mortgage, Inc.*, 635 F.3d 401, 422 (9th Cir.2011) ("We cannot conclude that the District Court abused its discretion or otherwise erred in ordering this [adverse inference jury instruction] sanction. Indeed, the District Court's sanction, which permits the jury to decide if any documents were destroyed when Johnson's hard drives were reformatted, strikes us as precisely the kind of flexible and resourceful sanction order that district judges should be encouraged to craft. We therefore affirm the sanction order.").

IV. CONCLUSION

The discovery process in our federal courts is anything but perfect. The burden to the parties and to the courts in cases such as this can be extraordinary. This court has previously imposed custodian limits, sampling requirements, and other measures to put at least some boundary around what has to date largely been an unbounded problem.[FN118] But it is no answer to that burden simply to leave in place an adjudicated spoliation tool and for seven months and take almost no steps to avoid spoliation beyond telling employees not to allow what will otherwise certainly happen. Nor can a party avoid any assessment whatsoever of the effect of the instruction it eventually puts into place. A modest, optional adverse jury instruction is the least restrictive means to remedy the prejudice from these past practices and deter such practices in the future. The court GRANTS–IN–PART Apple's motion for an adverse inference jury instruction.

FN118. *See, e.g., DCG Sys., Inc. v. Checkpoint Tech., LLC*, Case No. C–11–03792 PSG, 2011 WL 5244356, at *1 (N.D.Cal. Nov. 2, 2011) (setting forth restrictions on the amount of electronic document production, and noting that "[t]hese restrictions are designed to address the imbalance of benefit and burden resulting from email production in most cases"); *Perez v. State Farm Mut. Automobile Ins. Co.*, Case No. C–06–01962 JW (PSG), 2011 WL 2433393, at *1 (N.D.Cal. June 16, 2011) (identifying sampling as a less burdensome alternative to full-fledged document production).

IT IS SO ORDERED.

N.D.Cal.,2012.
Apple Inc. v. Samsung Electronics Co., Ltd.

881 F.Supp.2d 1132
(Cite as: 881 F.Supp.2d 1132)

881 F.Supp.2d 1132

END OF DOCUMENT

220 F.R.D. 212, 92 Fair Empl.Prac.Cas. (BNA) 1539
(Cite as: 220 F.R.D. 212)

United States District Court,
S.D. New York.
Laura ZUBULAKE, Plaintiff,
v.
UBS WARBURG LLC, UBS Warburg, and UBS AG, Defendants.

No. 02 Civ. 1243(SAS).
Oct. 22, 2003.

Background: In action by female employee under federal, state, and city law for gender discrimination, failure to promote, and retaliation, employee moved for sanctions against employer for its failure to preserve backup tapes containing potentially relevant e-mail correspondence of key employees.

Holdings: The District Court, Scheindlin, J., held that:
(1) employer had duty to preserve backup tapes;
(2) reconsideration of Court's prior cost-shifting order regarding backup tapes was not appropriate;
(3) adverse inference instruction was not warranted; but
(4) employer would be ordered to pay costs of deposing certain witnesses.

Motion granted in part.

West Headnotes

[1] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

"Spoliation" is the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation.

[2] Evidence 157 78

157 Evidence
157II Presumptions
157k74 Evidence Withheld or Falsified
157k78 k. Suppression or spoliation of evidence. Most Cited Cases

Spoliation of evidence germane to proof of an issue at trial can support an inference that the evidence would have been unfavorable to the party responsible for its destruction.

[3] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

Determination of an appropriate sanction for spoliation, if any, is confined to the sound discretion of the trial judge, and is assessed on a case-by-case basis.

[4] Federal Civil Procedure 170A 1636.1

220 F.R.D. 212, 92 Fair Empl.Prac.Cas. (BNA) 1539
(Cite as: 220 F.R.D. 212)

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

Authority to sanction litigants for spoliation arises jointly under the Federal Rules of Civil Procedure and the court's own inherent powers.

[5] Federal Civil Procedure 170A 1551

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)1 In General
170Ak1551 k. In general. Most Cited Cases

Obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.

[6] Federal Civil Procedure 170A 1551

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)1 In General
170Ak1551 k. In general. Most Cited Cases

In action by female employee for gender discrimination, failure to promote, and retaliation, employer had duty to preserve backup tapes containing potentially relevant e-mails which were not otherwise available and involved key employees; duty attached when relevant employees anticipated litigation, even though employee had not yet requested tapes or filed complaint.

[7] Federal Civil Procedure 170A 1551

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)1 In General
170Ak1551 k. In general. Most Cited Cases

As a general rule, a party need not preserve all backup tapes for e-mail even when it reasonably anticipates litigation.

[8] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

Anyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary.

[9] Federal Civil Procedure 170A 1551

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)1 In General
170Ak1551 k. In general. Most Cited Cases

While a litigant is under no duty to keep or retain every document in its possession, it is under a duty to

preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.

[10] Federal Civil Procedure 170A 1551

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)1 In General
170Ak1551 k. In general. Most Cited Cases

Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a litigation hold to ensure the preservation of relevant documents; as a general rule, that litigation hold does not apply to inaccessible e-mail backup tapes (e.g., those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy, but, on the other hand, if backup tapes are accessible (i.e., actively used for information retrieval), then such tapes would likely be subject to the litigation hold.

[11] Federal Civil Procedure 170A 1551

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)1 In General
170Ak1551 k. In general. Most Cited Cases

If a company can identify where particular employee documents are stored on e-mail backup tapes, then the tapes storing the documents of key players to existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available; this exception applies to all backup tapes.

[12] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

On motion by employee suing for gender discrimination, failure to promote, and retaliation, reconsideration of cost-shifting order, which directed parties to share cost of restoring certain backup tapes, was not appropriate remedy for employer's failure to preserve backup tapes containing potentially relevant and otherwise unavailable e-mail correspondence of key employees, since evidence that certain e-mails had not been retained and that certain backup tapes were missing had informed District Court's resolution of original cost-shifting motion.

[13] Federal Civil Procedure 170A 2173

170A Federal Civil Procedure
170AXV Trial
170AXV(G) Instructions
170Ak2173 k. Necessity and subject matter. Most Cited Cases

220 F.R.D. 212, 92 Fair Empl.Prac.Cas. (BNA) 1539
(Cite as: 220 F.R.D. 212)

Adverse inference instruction is an extreme sanction for spoliation of evidence and should not be given lightly.

[14] Federal Civil Procedure 170A 2173

170A Federal Civil Procedure
170AXV Trial
170AXV(G) Instructions
170Ak2173 k. Necessity and subject matter. Most Cited Cases

Party seeking an adverse inference instruction or other sanctions based on the spoliation of evidence must establish the following three elements: (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a culpable state of mind, including ordinary negligence, and (3) that the destroyed evidence was relevant to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense.

[15] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

When evidence is destroyed in bad faith (i.e., intentionally or willfully), that fact alone is sufficient to demonstrate relevance to support sanctions for spoliation of evidence; by contrast, when the destruction is negligent, relevance must be proven by the party seeking the sanctions.

[16] Federal Civil Procedure 170A 2173

170A Federal Civil Procedure
170AXV Trial
170AXV(G) Instructions
170Ak2173 k. Necessity and subject matter. Most Cited Cases

Even though employer had duty to preserve backup tapes, containing e-mail correspondence of key employees which was potentially relevant to female employee's suit for gender discrimination, failure to promote, and retaliation, and even though employer's destruction of certain backup tapes, covering time period when relevant employees anticipated litigation, was negligent, and of others, covering time period after employee filed Equal Employment Opportunity Commission (EEOC) charge, was grossly negligent, if not reckless, employer's spoliation did not warrant adverse inference instruction, absent evidence that destroyed evidence would have been favorable to employee.

[17] Evidence 157 78

157 Evidence
157II Presumptions
157k74 Evidence Withheld or Falsified
157k78 k. Suppression or spoliation of evidence. Most Cited Cases

In cases of negligent, grossly negligent, or reckless destruction of evidence, it cannot be inferred from the conduct of the spoliator that the evidence would even have been harmful to him; only in the case of willful spoliation is the spoliator's mental culpability itself evidence of the relevance of the documents destroyed.

[18] Federal Civil Procedure 170A 1637

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply

220 F.R.D. 212, 92 Fair Empl.Prac.Cas. (BNA) 1539
(Cite as: 220 F.R.D. 212)

170Ak1636 Failure to Comply; Sanctions
170Ak1637 k. Payment of expenses. Most Cited Cases

In action by female employee for gender discrimination, failure to promote, and retaliation, employer who destroyed potentially relevant backup tapes which it had duty to preserve would be required to pay costs for re-deposing certain witnesses for limited purpose of inquiring into issues raised by destruction of evidence and any newly discovered e-mails.

***214** James A. Batson, Liddle & Robinson, LLP, New York City, for Plaintiff.

Kevin B. Leblang, Norman C. Simon, Kramer Levin Naftalis & Frankel LLP, New York City, for Defendants.

OPINION AND ORDER

SCHEINDLIN, District Judge.

"Documents create a paper reality we call proof."[FN1] The absence of such documentary proof may stymie the search for the truth. If documents are lost or destroyed when they should have been preserved because a litigation was threatened or pending, a party may be prejudiced. The questions presented here are how to determine an appropriate penalty for the party that caused the loss and-the flip side-how to determine an appropriate remedy for the party injured by the loss.

FN1. Mason Cooley, *City Aphorisms, Sixth Selection* (1989).

Finding a suitable sanction for the destruction of evidence in civil cases has never been easy. Electronic evidence only complicates matters. As documents are increasingly maintained electronically, it has become easier to delete or tamper with evidence (both intentionally and inadvertently) and more difficult for litigants to craft policies that ensure all relevant documents are preserved.[FN2] This opinion addresses both the scope of a litigant's duty to preserve electronic documents and the consequences of a failure to preserve documents that fall within the scope of that duty.

FN2. *See* Adam I. Cohen & David J. Lender, *Electronic Discovery: Law and Practice* § 3.01 (Aspen Law & Business, publication forthcoming 2003) ("Unlike paper documents, electronic documents can be updated or changed without leaving an easily recognizable trace. Therefore, unique questions may arise as to the scope of a party's duty to preserve evidence in electronic form.").

I. BACKGROUND

This is the fourth opinion resolving discovery disputes in this case. Familiarity with ***215** the prior opinions is presumed,[FN3] and only background information relevant to the instant dispute is described here. In brief, Laura Zubulake, an equities trader who earned approximately $650,000 a year with UBS,[FN4] is suing UBS for gender discrimination, failure to promote, and retaliation under federal, state, and city law. She has repeatedly maintained that the evidence she needs to prove her case exists in e-mail correspondence sent among various UBS employees and stored only on UBS's computer systems.

FN3. *See Zubulake v. UBS Warburg, LLC,* 217 F.R.D. 309 (S.D.N.Y.2003) (*"Zubulake I"*) (addressing the legal standard for determining the cost allocation for producing e-mails contained on backup tapes); *Zubulake v. UBS Warburg, LLC,* No. 02 Civ. 1243, 2003 WL 21087136 (S.D.N.Y. May 13, 2003) (*"Zubulake II"*) (addressing Zubulake's reporting obligations); *Zubulake v. UBS Warburg LLC,* 216 F.R.D. 280 (S.D.N.Y.2003) (*"Zubulake III"*) (allocating backup tape restoration costs between Zubulake and UBS).

FN4. *See* 6/20/03 Letter from James A. Batson, Zubulake's counsel, to the Court.

220 F.R.D. 212, 92 Fair Empl.Prac.Cas. (BNA) 1539
(Cite as: 220 F.R.D. 212)

On July 24, 2003, I ordered the parties to share the cost of restoring certain UBS backup tapes that contained e-mails relevant to Zubulake's claims.[FN5] In the restoration effort, the parties discovered that certain backup tapes are missing. In particular:

FN5. *Zubulake III*, 216 F.R.D. 280.

Individual/Server	*Missing Monthly Backup Tapes*
Matthew Chapin (Zubulake's immediate supervisor)	April 2001
Jeremy Hardisty (Chapin's supervisor)	June 2001
Andrew Clarke and Vinay Datta (Zubulake's coworkers)	April 2001
Rose Tong (human resources)	Part of June 2001, July 2001, August 2001, and October 2001

(UBS has located certain *weekly* backup tapes to fill some of the gaps created by the lost monthly tapes).

In addition, certain isolated e-mails-created after UBS supposedly began retaining all relevant e-mails-were deleted from UBS's system, although they appear to have been saved on the backup tapes. As I explained in *Zubulake III*, "certain e-mails sent after the initial EEOC charge-and particularly relevant to Zubulake's retaliation claim-were apparently not saved at all. For example, [an] e-mail from Chapin to Joy Kim [another of Zubulake's coworkers] instructing her on how to file a complaint against Zubulake was not saved, and it bears the subject line 'UBS client attorney priviledge [sic] only,' although no attorney is copied on the e-mail. This potentially useful e-mail was deleted and resided only on UBS's backup tapes." [FN6]

FN6. *Zubulake III*, 216 F.R.D. at 287.

Zubulake filed her EEOC charge on August 16, 2001; the instant action was filed on February 14, 2002. In August 2001, in an oral directive, UBS ordered its employees to retain all relevant documents.[FN7] In August 2002, after Zubulake specifically requested e-mail stored on backup tapes, UBS's outside counsel orally instructed UBS's information technology personnel to stop recycling backup tapes.[FN8]

FN7. *See* 3/26/03 Oral Argument Transcript at 40 (Statement of Kevin Leblang, counsel to UBS) ("As of August when Ms. Zubulake filed a charge, everyone was told nothing gets deleted and we searched everyone's computer, everyone's hard files, the human resources files and the legal files.").

FN8. *See* 9/26/03 Oral Argument Transcript ("9/26/03 Tr.") at 18 (Statement of Norman C. Simon, counsel to UBS); *see also* 10/14/03 Letter from Norman Simon to the Court ("10/14/03 Ltr.") at 2.

Zubulake now seeks sanctions against UBS for its failure to preserve the missing backup tapes and deleted e-mails. In particular, Zubulake seeks the following relief: (a) an order requiring UBS to pay in full the costs of restoring the remainder of the monthly backup tapes; (b) an adverse inference instruction against UBS with respect to the backup tapes that are missing; and (c) an order directing UBS to bear the costs of re-deposing certain individuals, such as Chapin, ***216** concerning the issues raised in newly produced e-mails.

II. LEGAL STANDARD

[1][2][3][4] Spoliation is "the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." [FN9] The spoliation of evidence germane "to proof of an issue at trial can support an inference that the evidence would have been unfavorable to the party responsible for its destruction." [FN10] However, "[t]he determination of an appropriate sanction for spoliation, if any, is confined to the sound discretion of the trial judge, and is assessed on a case-by-case basis." [FN11] The authority to sanction litigants for spoliation arises jointly under the Federal Rules of Civil Procedure and the court's own inherent powers. [FN12]

FN9. *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir.1999).

FN10. *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir.1998).

FN11. *Fujitsu Ltd. v. Federal Express Corp.*, 247 F.3d 423, 436 (2d Cir.2001).

FN12. *See Turner v. Hudson Transit Lines, Inc.*, 142 F.R.D. 68, 72 (S.D.N.Y.1991)(Francis, M.J.) (citing Fed.R.Civ.P. 37). *See also Shepherd v. American Broadcasting Companies*, 62 F.3d 1469, 1474 (D.C.Cir.1995) ("When rules alone do not provide courts with sufficient authority to protect their integrity and prevent abuses of the judicial process, the inherent power fills the gap."); *id.* at 1475 (holding that sanctions under the court's inherent power can "include ... drawing adverse evidentiary inferences"). *See generally* Cohen & Lender, *supra* note 2, §§ 3.02[B][1]-[2].

III. DISCUSSION

It goes without saying that a party can only be sanctioned for destroying evidence if it had a duty to preserve it. If UBS had no such duty, then UBS cannot be faulted. I begin, then, by discussing the extent of a party's duty to preserve evidence.

A. Duty to Preserve

[5] "The obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation." [FN13] Identifying the boundaries of the duty to preserve involves two related inquiries: *when* does the duty to preserve attach, and *what* evidence must be preserved?

FN13. *Fujitsu*, 247 F.3d at 436 (citing *Kronisch*, 150 F.3d at 126). *See also Silvestri v. General Motors Corp.*, 271 F.3d 583, 591 (4th Cir.2001) ("The duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation.") (citing *Kronisch*, 150 F.3d at 126).

1. The Trigger Date

In this case, the duty to preserve evidence arose, at the latest, on August 16, 2001, when Zubulake filed her EEOC charge.[FN14] At that time, UBS's in-house attorneys cautioned employees to retain all documents, including e-mails and backup tapes, that could potentially be relevant to the litigation. [FN15] In meetings with Chapin, Clarke, Kim, Hardisty, John Holland (Chapin's supervisor), and Dominic Vail (Zubulake's former supervisor) held on August 29-31, 2001, UBS's outside counsel reiterated the need to preserve documents.[FN16]

FN14. *See* 9/26/03 Tr. at 16 (statement of Norman C. Simon agreeing that the duty to preserve attached no later than August 2001).

FN15. *See* 10/14/03 Ltr. and attached exhibits (reflecting correspondence from UBS's in-house counsel reiterating, in writing, the August 2001 oral directive to UBS employees to preserve documents).

220 F.R.D. 212, 92 Fair Empl.Prac.Cas. (BNA) 1539
(Cite as: 220 F.R.D. 212)

FN16. *See id.* at 1 n. 1.

But the duty to preserve may have arisen even before the EEOC complaint was filed. Zubulake argues that UBS "should have known that the evidence [was] relevant to future litigation," [FN17] as early as April 2001, and thus had a duty to preserve it. She offers two pieces of evidence in support of this argument. *First,* certain UBS employees titled e-mails pertaining to Zubulake "UBS Attorney Client Privilege" starting in April 2001, notwithstanding the fact that no attorney was copied on the e-mail and the ***217** substance of the e-mail was not legal in nature. *Second,* Chapin admitted in his deposition that he feared litigation from as early as April 2001:

FN17. *Fujitsu,* 247 F.3d at 436.

Q: Did you think that Ms. Zubulake was going to sue UBS when you received these documents?

A: What dates are we talking about?

Q: Late April 2001.

A: Certainly it was something that was in the back of my head.[FN18]

FN18. 2/12/03 Deposition of Matthew Chapin at 247:14-247:19, Ex. B. to the 9/15/03 Letter from James Batson to the Court ("Batson Ltr.").

[6] Merely because one or two employees contemplate the possibility that a fellow employee might sue does not generally impose a firm-wide duty to preserve. But in this case, it appears that almost everyone associated with Zubulake recognized the possibility that she might sue. For example, an e-mail authored by Zubulake's co-worker Vinnay Datta, concerning Zubulake and labeled "UBS attorney client priviladge [sic]," was distributed to Chapin (Zubulake's supervisor), Holland and Leland Tomblick (Chapin's supervisor), Vail (Zubulake's former supervisor), and Andrew Clarke (Zubulake's co-worker) in late April 2001.[FN19] That e-mail, replying to one from Hardisty, essentially called for Zubulake's termination: "Our biggest strength as a firm and as a desk is our ability to share information and relationships. Any person who threatens this in any way should be firmly dealt with.... [B]elieve me that a lot of other [similar] instances have occurred earlier." [FN20]

FN19. *See* 4/27/01 e-mail, Ex. A to Batson Ltr.

FN20. *Id.*

Thus, the relevant people at UBS anticipated litigation in April 2001. The duty to preserve attached at the time that litigation was reasonably anticipated.

2. Scope

[7] The next question is: What is the scope of the duty to preserve? Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every e-mail or electronic document, and every backup tape? The answer is clearly, "no". Such a rule would cripple large corporations, like UBS, that are almost always involved in litigation.[FN21] As a general rule, then, a party need not preserve all backup tapes even when it reasonably anticipates litigation.[FN22]

FN21. *Cf. Concord Boat Corp. v. Brunswick Corp.*, No. LR-C-95-781, 1997 WL 33352759, at *4 (E.D.Ark. Aug. 29, 1997) ("to hold that a corporation is under a duty to preserve all e-mail potentially relevant to any future litigation would be tantamount to holding that the corporation must preserve all e-mail.... Such a proposition is not justified.").

FN22. *See, e.g., The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery* cmt 6.h (Sedona Conference Working Group Series

2003) ("Absent specific circumstances, preservation obligations should not extend to disaster recovery backup tapes....").

[8][9] At the same time, anyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary. "While a litigant is under no duty to keep or retain every document in its possession ... it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request." [FN23]

FN23. *Turner,* 142 F.R.D. at 72 (quoting *William T. Thompson Co. v. General Nutrition Corp.,*593 F.Supp. 1443, 1455 (C.D.Cal.1984)).

i. Whose Documents Must Be Retained?

The broad contours of the duty to preserve are relatively clear. That duty should certainly extend to any documents or tangible things (as defined by Rule 34(a)) [FN24] made by ***218** individuals "likely to have discoverable information that the disclosing party may use to support its claims or defenses." [FN25] The duty also includes documents prepared *for* those individuals, to the extent those documents can be readily identified (*e.g.*, from the "to" field in e-mails). The duty also extends to information that is relevant to the claims or defenses of *any* party, or which is "relevant to the subject matter involved in the action."[FN26] Thus, the duty to preserve extends to those employees likely to have relevant information-the "key players" in the case. In this case, all of the individuals whose backup tapes were lost (Chapin, Hardisty, Tong, Datta and Clarke) fall into this category. [FN27]

FN24. *See* Fed.R.Civ.P. 34(a) (defining the term "document" to "includ[e] writings, drawings, graphs, charts, photographs, phonorecords, and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form"); *see also Zubulake I,* 217 F.R.D. at 316-17 (holding that the term "document," within the meaning of Rule 34(a), includes e-mails contained on backup tapes).

FN25. Fed.R.Civ.P. 26(a)(1)(A).

FN26. Fed.R.Civ.P. 26(b)(1).

FN27. *See* 9/26/03 Tr. at 17 (Statement of Norman C. Simon agreeing that the duty to preserve applied to the documents' of Chapin, Hardisty, Tong, Datta and Clarke).

ii. What Must Be Retained?

A party or anticipated party must retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches, and any relevant documents created thereafter. In recognition of the fact that there are many ways to manage electronic data, litigants are free to choose how this task is accomplished. For example, a litigant could choose to retain all then-existing backup tapes for the relevant personnel (if such tapes store data by individual or the contents can be identified in good faith and through reasonable effort), and to catalog any later-created documents in a separate electronic file. That, along with a mirror-image of the computer system taken at the time the duty to preserve attaches (to preserve documents in the state they existed at that time), creates a complete set of relevant documents. Presumably there are a multitude of other ways to achieve the same result.

iii. Summary of Preservation Obligations

[10] The scope of a party's preservation obligation can be described as follows: Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents. As a general rule, that litigation hold does not apply to inaccessible backup tapes (*e.g.*, those typically maintained solely for the purpose of disaster recovery), which may

continue to be recycled on the schedule set forth in the company's policy. On the other hand, if backup tapes are accessible (*i.e.*, actively used for information retrieval), then such tapes *would* likely be subject to the litigation hold.

[11] However, it does make sense to create one exception to this general rule. If a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of "key players" to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available. This exception applies to *all* backup tapes.

iv. What Happened at UBS After August 2001?

By its attorney's directive in August 2002, UBS endeavored to preserve all backup tapes that existed in August 2001 (when Zubulake filed her EEOC charge) that captured data for employees identified by Zubulake in her document request, and all such monthly backup tapes generated thereafter. These backup tapes existed in August 2002, because of UBS's document retention policy, which required retention for three years.[FN28] In August 2001, UBS employees were instructed to maintain *active* electronic documents pertaining to Zubulake in separate files.[FN29] Had these directives been followed, UBS would have met its preservation obligations by preserving one copy of all relevant documents ***219** that existed at, or were created after, the time when the duty to preserve attached.

FN28. *See Zubulake I*, 217 F.R.D. at 314 ("Nightly backup tapes were kept for twenty working days, weekly tapes for one year, and monthly tapes for three years.").

FN29. *See Zubulake III*, 216 F.R.D. at 287.

In fact, UBS employees did not comply with these directives. Three backup tapes containing the e-mail files of Chapin, Hardisty, Clarke and Datta created after April 2001 were lost, despite the August 2002 directive to maintain those tapes. According to the UBS document retention policy, these three monthly backup tapes from April and June 2001 should have been retained for three years.[FN30]

FN30. *See supra* note 28. According to a chart prepared by UBS's attorneys and presented during oral arguments, the three backup tapes of U.S. personnel were in fact deleted between October 2001 and February 2002-after UBS staff were warned to retain documents, but before they were told specifically to preserve backup tapes.

The two remaining lost backup tapes were for the time period *after* Zubulake filed her EEOC complaint (Rose Tong's tapes for August and October 2001). UBS has offered *no* explanation for why these tapes are missing. UBS initially argued that Tong is a Hong Kong based UBS employee and thus her backup tapes "are not subject to any internal retention policy." [FN31] However, UBS subsequently informed the Court that there *was* a document retention policy in place in Hong Kong starting in June 2001, although it only required that backup tapes be retained for one month.[FN32] It also instructed employees "not [to] delete any emails if they are aware that ... litigation is pending or likely, or during ... a discovery process."[FN33] In any event, it appears that UBS did not directly order the preservation of Tong's backup tapes until August 2002, when Zubulake made her discovery request.[FN34]

FN31. 9/17/03 Letter from Kevin Leblang to the Court ("Leblang Ltr.").

FN32. *See* 10/14/03 Ltr. at 2-3; *see also* UBS Asia policy for "Retention of Back-up Tapes of Email Servers," ("UBS Asia Policy") Ex. F to 10/14/03 Ltr.

FN33. UBS Asia Policy at 2.

FN34. *See* 9/26/03 Tr. at 31, 35-36.

220 F.R.D. 212, 92 Fair Empl.Prac.Cas. (BNA) 1539
(Cite as: 220 F.R.D. 212)

In sum, UBS had a duty to preserve the six-plus backup tapes (that is, six complete backup tapes and part of a seventh) at issue here.

B. Remedies

As noted, Zubulake has requested three remedies for UBS's spoliation of evidence. I consider each remedy in turn.

1. Reconsideration of the Cost-Shifting Order

[12] Zubulake's request that this Court re-consider its July 24, 2003, Order in *Zubulake III* is inappropriate. At the time that motion was made, the Court was well aware that certain e-mails had not been retained and that certain backup tapes were missing.[FN35] Indeed, Zubulake urged that these missing backup tapes "be considered as a factor in why the costs should be shifted to defendants," in part because she would have chosen one of the lost tapes as part of the court-ordered sample restoration.[FN36] And these lost tapes and deleted e-mails did, in fact, inform my resolution of the cost-shifting motion. In *Zubulake III*, in my analysis of the marginal utility factors, I specifically noted that "there is some evidence that Chapin was concealing and deleting especially relevant e-mails."[FN37] There is therefore no need to reconsider that ruling in light of the instant motion; this evidence already played a role in the cost-shifting decision.

FN35. *See* 9/26/03 Tr. at 27.

FN36. 6/17/03 Oral Argument Transcript (Statement of James Batson).

FN37. 216 F.R.D. at 287.

2. Adverse Inference

[13] Zubulake next argues that UBS's spoliation warrants an adverse inference instruction. Zubulake asks that the jury in this case be instructed that it can infer from the fact that UBS destroyed certain evidence that the evidence, if available, would have been favorable to Zubulake and harmful to UBS. In practice, an adverse inference instruction often ends litigation-it is too difficult a hurdle for the spoliator to overcome. The *in terrorem* effect of an adverse inference is obvious. When a jury is instructed that it may "infer that the party who destroyed ***220** potentially relevant evidence did so 'out of a realization that the [evidence was] unfavorable,' "[FN38] the party suffering this instruction will be hard-pressed to prevail on the merits. Accordingly, the adverse inference instruction is an extreme sanction and should not be given lightly.[FN39]

FN38. *Linnen v. A.H. Robins Co.*, No. 97-2307, 1999 WL 462015, at *11 (Mass.Super. June 16, 1999) (alteration in original) (quoting *Blinzler v. Marriott International, Inc.*, 81 F.3d 1148, 1158 (1st Cir.1996)).

FN39. *See* Mary Kay Brown & Paul D. Weiner, *Digital Dangers: A Primer on Electronic Evidence in the Wake of Enron*, 74 Pa. B.A.Q. 1, 7 (2003) (listing "severe sanctions, such as adverse inference instructions" imposed by courts when "relevant electronic evidence was not preserved, or was intentionally destroyed"); *but see Mosel Vitelic Corp. v. Micron Technology, Inc.*, 162 F.Supp.2d 307, 315 (D.Del.2000) ("adverse inference instructions are one of the least severe sanctions which the court can impose").

[14][15] A party seeking an adverse inference instruction (or other sanctions) based on the spoliation of evidence must establish the following three elements: (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a "culpable state of mind" and (3) that the destroyed evidence was "relevant" to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense.[FN40] In this circuit, a "culpable state of mind" for purposes of a spoliation inference includes ordinary negligence.[FN41] When evidence is destroyed in bad faith (*i.e.*, intentionally or willfully), that fact alone is sufficient to demonstrate relevance.[FN42] By contrast, when the destruc-

tion is negligent, relevance must be proven by the party seeking the sanctions.[FN43]

FN40. *Byrnie v. Town of Cromwell,* 243 F.3d 93, 107-12 (2d Cir.2001).

FN41. *See Residential Funding Corp. v. DeGeorge Fin. Corp.,* 306 F.3d 99, 108 (2d Cir.2002).

FN42. *See id.* at 109.

FN43. *See id.*

a. Duty to Preserve

[16] For the reasons already discussed, UBS had-and breached-a duty to preserve the backup tapes at issue. Zubulake has thus established the first element.

b. Culpable State of Mind

Zubulake argues that UBS's spoliation was "intentional-or, at a minimum, grossly negligent." [FN44] Yet, of dozens of relevant backup tapes, only six and part of a seventh are missing. Indeed, UBS argues that the tapes were "inadvertently recycled well before plaintiff requested them and even before she filed her complaint [in February 2002]." [FN45]

FN44. *See* Batson Ltr. at 2.

FN45. Leblang Ltr. at 2.

But to accept UBS's argument would ignore the fact that, even though Zubulake had not yet requested the tapes or filed her complaint, UBS had a duty to preserve those tapes. Once the duty to preserve attaches, any destruction of documents is, at a minimum, negligent.[FN46] (Of course, this would not apply to destruction caused by events outside of the party's control, *e.g.,* a fire in UBS's offices).

FN46. *See* Black's Law Dictionary (6th ed.1991) (defining "negligence" as "that legal delinquency which results whenever a man fails to exhibit the care which he ought to exhibit, whether it be slight, ordinary, or great. It is characterized chiefly by inadvertence, thoughtlessness, inattention, and the like...."). *Cf. Keir v. Unumprovident Corp.,* No. 02 Civ. 8781, 2003 WL 21997747, at *13 (S.D.N.Y. Aug.22, 2003) (criticizing defendant for loss of e-mails even though loss occurred "through the fault of no one," because "[i]f UnumProvident had been as diligent as it should have been ... many fewer [backup] tapes would have been inadvertently overwritten.").

Whether a company's duty to preserve extends to backup tapes has been a grey area. As a result, it is not terribly surprising that a company would think that it did *not* have a duty to preserve all of its backup tapes, even when it reasonably anticipated the onset of litigation. Thus, UBS's failure to preserve all potentially relevant backup tapes was merely negligent, as opposed to grossly negligent or reckless.[FN47]

FN47. Litigants are now on notice, at least in this Court, that backup tapes that can be identified as storing information created by or for "key players" must be preserved.

***221** UBS's destruction or loss of Tong's backup tapes, however, exceeds mere negligence. UBS failed to include these backup tapes in its preservation directive in this case, notwithstanding the fact that Tong was the human resources employee directly responsible for Zubulake and who engaged in continuous correspondence regarding the case. Moreover, the lost tapes covered the time period *after* Zubulake filed her EEOC charge, when UBS was *unquestionably* on notice of its duty to preserve. Indeed, Tong herself took part in much of the correspondence over Zubulake's charge of discrimination. Thus, UBS was grossly negligent, if not reckless, in not preserving those backup tapes.

Because UBS was negligent-and possibly reckless-Zubulake has satisfied her burden with respect to the second prong of the spoliation test.

c. Relevance

[17] Finally, because UBS's spoliation was negligent and possibly reckless, but not willful, Zubulake must demonstrate that a reasonable trier of fact could find that the missing e-mails would support her claims.[FN48] In order to receive an adverse inference instruction, Zubulake must demonstrate not only that UBS destroyed relevant evidence as that term is ordinarily understood,[FN49] but also that the destroyed evidence would have been favorable to her.[FN50] "This corroboration requirement is even more necessary where the destruction was merely negligent, since in those cases it cannot be inferred from the conduct of the spoliator that the evidence would even have been harmful to him." [FN51] This is equally true in cases of gross negligence or recklessness; only in the case of *willful* spoliation is the spoliator's mental culpability itself evidence of the relevance of the documents destroyed.[FN52]

FN48. *See Byrnie*, 243 F.3d at 107-12.

FN49. *See* Fed.R.Evid. 401; Fed.R.Civ.P. 26(b)(1)

FN50. *See Residential Funding*, 306 F.3d at 108-09 ("Although we have stated that, to obtain an adverse inference instruction, a party must establish that the unavailable evidence is 'relevant' to its claims or defenses, our cases make clear that 'relevant' in this context means something more than sufficiently probative to satisfy Rule 401 of the Federal Rules of Evidence. Rather, the party seeking an adverse inference must adduce sufficient evidence from which a reasonable trier of fact could infer that 'the destroyed or unavailable evidence would have been of the nature alleged by the party affected by its destruction.' ") (citations, footnote, and alterations omitted).

FN51. *Turner*, 142 F.R.D. at 77 (citing *Stanojev v. Ebasco Services, Inc.*, 643 F.2d 914, 924 n. 7 (2d Cir.1981)).

FN52. *See Residential Funding*, 306 F.3d at 109.

On the one hand, I found in *Zubulake I* and *Zubulake III* that the e-mails contained on UBS's backup tapes were, by-and-large, relevant in the sense that they bore on the issues in the litigation.[FN53] On the other hand, *Zubulake III* specifically held that "nowhere (in the sixty-eight e-mails produced to the Court) is there evidence that Chapin's dislike of Zubulake related to her gender." [FN54] And those sixty-eight e-mails, it should be emphasized, were the ones selected by Zubulake as being the *most* relevant among all those produced in UBS's sample restoration. There is no reason to believe that the lost e-mails would be any more likely to support her claims.

FN53. *See Zubulake I*, 217 F.R.D. at 316-17; *Zubulake III*, 216 F.R.D. at 284-87.

FN54. 216 F.R.D. at 286.

Furthermore, the likelihood of obtaining relevant information from the six-plus lost backup tapes at issue here is even lower than for the remainder of the tapes, because the majority of the six-plus tapes cover the time prior to the filing of Zubulake's EEOC charge. The tape that is most likely to contain relevant e-mails is Tong's August 2001 tape-the tape for the very month that Zubulake filed her EEOC charges. But the majority of the e-mails on that tape are preserved on the September 2001 tape. Thus, there is no reason to believe that peculiarly unfavorable evidence resides solely on that missing tape. Accordingly, Zubulake has not sufficiently demonstrated that the lost tapes contained relevant information.[FN55]

FN55. *See generally Turner*, 142 F.R.D. at 77 ("Where, as here, there is no extrinsic evidence whatever tending to show that the destroyed

> evidence would have been unfavorable to the spoliator, no adverse inference is appropriate."); *Concord Boat Corp. v. Brunswick Corp.*, 1997 WL 33352759, at *7 (E.D.Ark.1997) ("It would simply be inappropriate to give an adverse inference instruction based upon speculation that deleted e-mails would be unfavorable to Defendant's case.").

***222 d. Summary**

In sum, although UBS had a duty to preserve all of the backup tapes at issue, and destroyed them with the requisite culpability, Zubulake cannot demonstrate that the lost evidence would have supported her claims. Under the circumstances, it would be inappropriate to give an adverse inference instruction to the jury.

3. UBS Must Pay the Costs of Additional Depositions

[18] Even though an adverse inference instruction is not warranted, there is no question that e-mails that UBS should have produced to Zubulake were destroyed by UBS. That being so, UBS must bear Zubulake's costs for re-deposing certain witnesses for the limited purpose of inquiring into issues raised by the destruction of evidence and any newly discovered e-mails. In particular, UBS is ordered to pay the costs of re-deposing Chapin, Hardisty, Tong, and Josh Varsano (a human resources employee in charge of the Asian Equities Sales Desk and known to have been in contact with Tong during August 2001).[FN56]

> FN56. *See* 9/26/03 Tr. at 26 (statement of James Batson, seeking to re-depose only these four employees).

IV. CONCLUSION

For the reasons set forth above, Zubulake's motions for an adverse inference instruction and for reconsideration of the Court's July 24, 2003, Order are denied. Her motion seeking costs for additional depositions is granted.

SO ORDERED.

S.D.N.Y.,2003.
Zubulake v. UBS Warburg LLC
220 F.R.D. 212, 92 Fair Empl.Prac.Cas. (BNA) 1539

END OF DOCUMENT

Not Reported in F.Supp.2d, 2013 WL 6486921 (S.D.Ill.)
(Cite as: 2013 WL 6486921 (S.D.Ill.))

H

Only the Westlaw citation is currently available.

United States District Court, S.D. Illinois.
In re Pradaxa (Dabigatran Etexilate) Products Liability Litigation
This Document Relates to All Cases

MDL No. 2385
3:12–md–02385–DRH–SCW
Filed December 9, 2013

CASE MANAGEMENT ORDER NUMBER 50
Regarding the PSC's Second Motion for Sanctions (Doc. 302)

HERNDON, Chief Judge:

I. INTRODUCTION

***1** Presently before the Court is the PSC's motion seeking sanctions against Boehringer Ingelheim International GMBH ("BII") and Boehringer Ingelheim Pharmaceuticals, Inc. ("BIPI") (collectively, "the defendants") for various alleged discovery abuses (Doc. 302). The defendants filed a responsive brief on November 26, 2013 (Doc. 311). The Court heard oral argument on the motion on December 2, 2013. During oral argument, the defendants requested leave to file a supplemental response to address any new information alleged by the PSC during the hearing. The request for leave was granted and the defendants filed their supplemental brief on December 4, 2013 (Doc. 317).

The PSC's motion for sanctions addresses alleged discovery violations that fall into one of four categories: (1) the defendants' failure to preserve the custodial file of Professor Thorstein Lehr (a high-level scientist formerly employed by BII intricately involved in Pradaxa), as well as the failure to identify Prof. Lehr as a custodian with potentially relevant evidence; (2) the defendants' failure to preserve evidence relating to and/or untimely disclosure and production of material in the possession of the defendants' Sales Representatives, Clinical Science Consultants and Medical Science Liaisons; (3) the production issues related to the G Drive (one of the defendants' shared networks); and (4) the failure to preserve and/or untimely production of business related text messages on certain employees' cell phones.

A number of the alleged discovery violations are tied to the defendants' duty to preserve evidence relevant to this litigation and the gross inadequacy of the litigation hold that has been adopted by the defendants' to date. In the instant case, the defendants' preservation obligation was triggered in February of 2012 (as to BIPI) and, at the latest, April 2012 (as to BII). Further, there is no question that, as of June 2012, both defendants knew that nationwide Pradaxa product liability litigation, involving hundreds of cases, was imminent. Thus, while the defendants may have been able to justify adopting a narrow litigation hold as to *some* employees prior to June 2012, [FN1] they cannot justify failing to adopt a company-wide litigation hold as of June 2012—when they knew nationwide Pradaxa product liability litigation was imminent.

FN1. For instance, when only one or two cases had been filed (assuming the defendants did not know or did not have reason to know that nationwide litigation was imminent), it may have been appropriate to limit the litigation hold as to sales representatives (for example) to those sales representatives detailing Pradaxa in the same region where the subject plaintiff received his or her prescription for Pradaxa. However, even with

> just a few cases on file, the defendants' would have owed a duty to preserve the custodial files of top Pradaxa scientists (for example) as such information could be potentially relevant to any individual plaintiff's Pradaxa product liability action.

II. BACKGROUND DISCOVERY ABUSES

A. Cumulative Effect of Ongoing Discovery Abuses

***2** Unfortunately, this is not the defendants' first instance of discovery issues or having to answer serious allegations of discovery abuse and defend requests for court sanctions. Almost since its inception, this litigation has been plagued with discovery problems primarily associated with misconduct on the part of the defendants. The Court is continuously being called upon to address issues relating to untimely, lost, accidentally destroyed, missing, and/or "just recently discovered" evidence. The defendants' justifications for these discovery violations include but are not limited to the following: (1) placing the blame on others such as third-party vendors (production is delayed due to "vendor issues"), their own IT departments (we told IT to give the vendors full access to the database but for some reason IT provided the vendors with limited access), their own employees (the defendants' deponent did not understand that work related day planners should have been produced or the employees did not understand that work related text messages should have been retained and produced); (2) the defendants' and/or counsel's lack of experience in addressing litigation of this size; (3) the defendants' did not know, until recently, that this would turn into a large nationwide MDL; (4) unusual technical issues (despite our best efforts, that employee's hard drive was accidentally erased during a routine windows 7 update); (5) minimizing the alleged abuses (yes, we failed to produce this database but it was only 500,000 pages of documents compared to the 3 million we already produced or yes that material was accidentally destroyed but the PSC doesn't really need it); (6) blaming the PSC for submitting too many discovery requests that are broad in scope (only as an excuse after discovery violations are alleged but never as a proactive motion to limit discovery); and (7) the defendants' did not know about the "gaps" in their production until they began a comprehensive recheck or audit of the discovery process in September 2013.

The Court has been exceedingly patient and, initially, was willing to give the defendants the benefit of the doubt as to these issues. However, as the Court has warned the defendants in the past, when such conduct continues, there is a cumulative effect that the Court not only can but should take into account. Accordingly, the Court initially reviews the issues that have arisen to date.

B. Discovery Issues Preceding the PSC's First Motion for Sanctions

1. History of Discovery Abuses Outlined in the PSC's First Motion for Sanctions

The PSC's first motion for sanctions provides an overview of the discovery issues that had arisen as of the date of its filing (September 11, 2013) (Doc. 266). The Court will not recount all of the discovery issues detailed in that motion and instead incorporates them by reference. The Court also incorporates by reference the defendants' response to that motion (Doc. 271). The Court notes, however, that, for the most part, it agrees with and adopts the list of discovery abuses as detailed by the PSC. Further, with regard to the discovery issues that had arisen as of September 2013, the Court specifically notes the matters outlined below.

2. Cancellation of Depositions to Allow Defendants to Get Their House in Order

At the status conference on June 10, 2013 the Court cancelled approximately two months of depositions. In a subsequent Case Management Order, the

Court reflected on the cancellations as follows:

> At the status conference on June 10, 2013, the Court approved the parties' request to cancel approximately two months of depositions. The cancellation was necessitated by a number of document production deficiencies in relation to the custodial files of former and present BIPI and BII employees identified by the PSC as deponents. The parties indicated that, in light of the document production deficiencies, the custodial depositions should be delayed to allow the defendants to get their house in order and to ensure that the PSC had complete custodial files prior to taking the subject depositions. The parties further represented that the depositions could be cancelled and rescheduled without delaying the bellwether trial dates already in place. The Court concluded the requested cancellation was in the best interest of the litigation and directed the parties to confer and negotiate a revised document production and pretrial schedule that maintained the bellwether trial dates already in place.
>
> (CMO 38, Doc. 231 p. 1)

3. CMO 38 and the Court's Findings Regarding Certain Discovery Abuses

The PSC alerted the Court to problematic supplemental custodial file productions that included thousands of pages of "old" documents (documents that should have already been produced) and the production of otherwise incomplete custodial files. The Court found, in relevant part, as follows:

> Although some of the supplemental productions may have been made for legitimate reasons (vendor issues, technical problems, supplemental privilege review), the Court takes issue with the lack of transparency in alerting the Court or the PSC to matters that delayed the production of complete custodial files on the dates ordered by this Court. In general, the Court finds that BIPI failed to timely produce or timely respond to discovery as outlined by the plaintiffs letter-brief.
>
> ***3** In addition, the Court is particularly concerned with what appears to be a unilateral decision by BIPI to withhold "highly confidential" documents from the custodial files of non-German custodians—without informing the Court or the PSC that such documents were being withheld.... BIPI's unilateral decision to do so violated this Court's orders. Considering the above, the Court finds that BIPI inappropriately withheld "highly confidential" documents contrary to its agreement with the PSC and with this Court's orders.

(CMO 38, Doc. 231 pp. 5–8). As a result of the Court's findings, the Court adopted a revised production schedule (CMO 37, Doc. 230). Further, the Court imposed a certification requirement on BIPI and BII (CMO 38, Doc. 231 p. 8). The certification required both defendants "to provide a certification attesting to the completeness of productions."

C. The Court's Ruling Regarding the PSC's First Motion for Sanctions

On September 18, 2013, after hearing oral argument on the PSC's first motion for sanctions, the Court ruled from the bench. The following are relevant excerpts from that ruling:

> The Court finds here today that the defendant has violated or failed to meet either the letter or spirit of the Court's orders relative to discovery in a number of respects. It's hard for the Court, in this context and on this record to determine exactly where the fault lies in relation to the questions that I gave to Mr. Schmidt. I am not provided with the information. As I asked Mr. Schmidt, there could be outright deliberate violation of the order for the purpose of delaying production. It could be that there is gross negligence on the part of employees.

There could be a failure of leadership at BIPI or BII in failing to make the employees understand their responsibilities.

The upshot is, however, that the defendants have simply failed to follow the Court's orders. I agree with the list that was—I asked the plaintiffs to provide a list of what they thought were failures on the part of the defendants. I agree with that list, adopt it for the purpose of this order. I find for the remedy that I will fashion that I need not rule upon the motive that the plaintiffs suggest, but I also agree and find that there have been the additional violations since September 11, the five that Mr. Katz set out. I have in my notes the entire list, but for purposes of this order I'll simply adopt the list by reference. They're so numerous, which is one of the things that's so distressing to me.

(Doc. 277 p. 92 l. 23–p. 93 l. 22)

I've never seen a litigation where the problems are just ongoing and continual, and every month or every week there's an issue of this failure and that failure and the other failure. It just is astounding. The reason, that it's because of the volume or because of the scope or because of the breadth or because of the this or that, the vendor or this other or that other, that's fine in the early going perhaps but as the litigation matures the reasons just don't make sense and just simply can't be tolerated by the Court.

So it finally got to the point where we last met on September the 4th where I simply drew a line and said, The next time I hear of a failure we're going to talk about this in court with employees from the defendants, and it just took a matter of a few hours before I heard about the next failure. So there simply has to be a way to make this stop and to resolve once and for all this issue of failure after failure, and, in my eyes, violation after violation after violation of this Court's orders. It gets to the point where, from the Court's viewpoint, it's not simply working through rough patches and how to handle litigation, but a simple disregard of the Court's orders regardless of the motivation.

***4** So throughout these countless discussions over these issues and defendants' counsel doing everything they could to try to minimize the overall impact of these violations, the Court has just become frustrated beyond comprehension with these violations, some causing delays, some causing extraordinary delays, others just simply being glitches in the process of trying to get these cases in a posture to either be tried or resolved. And the ultimate goal, of course, giving the medical community an answer to this issue, giving the defendant an answer to this issue, giving the plaintiffs an answer to the issues, and performing the duties that we're all here to perform.

My conclusion, therefore—and I agree with the plaintiffs. I'm not sure if Mr. Katz kept count of the number of times they used “totality” or not, as he did with the defendant's use of words, but I agree that the totality of the circumstance here is and the totality of the violations is what counts. If you violate a Court order and remedy it, you don't get to start from scratch as far as I'm concerned. Your conduct is what it is, and if the conduct continues it's—there is a cumulative effect that the Court not only can but should take into account as time goes on.

And so my finding and conclusion is that there has been a clear pattern of numerous and substantial violations of the Court's many orders that have occurred in the past. I believe these have prejudiced the Court prejudiced the plaintiffs, I'm sorry, and have held this Court and demonstrated a holding of this Court in low regard, and they have amounted to a contumacious disregard for its authority. Under Rule 37 and the Court's inherent authority, I have available to me a number of options, one of which, of course, is the option which the plaintiffs

seek, which is to strike the defendant's pleadings in whole or in part. It's my finding that that is an option which is too draconian. I will not exercise my discretion in that regard. If this were a single plaintiff and a single defendant, perhaps that would be an appropriate response, but I choose not to exercise my option in that regard. However, I find that an appropriate response would be a couple of things: One, to impose a fine on the defendant, and two, to impose certain mandatory injunctions on the defendant. And my order is as follows:

In accordance with my inherent authority, in accordance with Rule 37, I hereby sanction the defendants by ordering them to pay a fine in the registry of this court in the amount of $29,540. For anybody that's done the math quickly, that amounts to $20 per case, not a very drastic amount, I don't believe. However, the defendant should understand I also believe in progressive discipline should this Court have to visit this issue again.

I further order the defense counsel, together with the five officers who appeared here today, to oversee a communication to all known witnesses—and this is the mandatory injunction part—and custodians of every known or potential source of discoverable material to do an immediate search for any yet undisclosed materials that are relevant in the broadest possible definition of that word to this litigation and to advise counsel of its existence by Monday of next week.

I understand you said you've been conducting an audit, but I absolutely do not know what that consists of, but I want some sort of communication from you folks that are involved in overseeing of this litigation something in writing that makes it quite clear to everybody that has some sort of control over discoverable material, so they have no way to mistake their duties and obligations, to make sure they search their records high and low for anything that's discoverable, and to report their results by Monday. If any—a witness or custodian is not present at the place where they maintain such records or discoverable material, they're to do so within two days of returning to said location, if they're on vacation, they're out of the office, whatever that circumstance may be.

***5** The communication which conveys this instruction shall describe in detail what is required of the witness or custodian and shall provide the name and contact information of a person with specific legal knowledge whom the witness or custodian may communicate with for information in the event he or she has any questions about what must be disclosed. The communication must also suggest that any individual questions of inclusion—in other words, if they wonder whether a matter of material is discoverable or not, should be resolved on the side of assuming that disclosure to counsel is the best course, and counsel can thereafter examine the material for exclusion, if appropriate. This may have already been done. Mr. Schmidt referred to it in his argument, but for depositions in the past that were cancelled as a result—this continues with a mandatory injunction part. For depositions in the past that were cancelled as a result of the defendants' failure to timely produce documents and for which defendants have not already agreed to reimburse, the plaintiffs may petition the Court to have their expenses reimbursed by defendants for appearing if no part of the deposition took place. In such event, expenses of Judge Stack will be borne solely by the defendant. For future depositions, should a deposition be cancelled due to the failure of defendants to timely produce material which it was required to produce, and no part of the deposition was taken, plaintiffs may petition the Court to have their expenses reimbursed by defendants. In such event expenses of Judge Stack shall be borne solely by the defendants. Once again, if defendants agree to the reimbursement, plaintiffs need not petition the Court.

In the event of a petition by plaintiffs for reimbursement, plaintiffs shall provide the Court with detail regarding the reason for the reimbursement, an itemization for the expenses they seek reimbursement, and shall include—for the expenses they seek for reimbursement. Plaintiffs shall forward a copy to defendants, who shall have 14 days to respond. If they intend to contest the request, that is, if the Court grants the request, the action by the Court automatically means Judge Stack's expenses for the cancelled deposition shall be borne solely by the defendant.

As a further mandatory injunction, should a scheduled deposition be cancelled due to an alleged failure of defendants to abide by discovery order of this Court and is the only deposition scheduled for that location, whether that venue is outside or within the United States, the parties are hereby directed to submit the facts of the occurrence to the Court within seven days of its occurrence. In addition to the facts, the parties will submit to the Court the available dates they suggest the deposition should be reset, given the need to examine the late-filed material and the upcoming deposition schedules, together with the names of the likely lead interrogators for the deposition. Court will then select a date for the scheduled—for rescheduling the deposition and will select a venue for the deposition, most likely the city of the main office of the lead interrogator, or St. Louis, as the Court determines is the reasonable location.

Should the defendants continue to violate discovery orders this Court has entered, the Court will consider, on motion by the plaintiffs or its own motion, further sanctions, including all sanctions authorized by Federal Rule of Civil Procedure 37, or its inherent authority. Furthermore, if the Court is forced to hold such a hearing the defendant can expect to produce at that hearing certain employees as designated by the Court, pursuant to its inherent authority, for testimony so that the Court can determine the nature of defendants' good faith in complying with the Court's order announced today, as well as their good faith in complying with the discovery orders generally in this litigation.

(Doc. 277 p. 95 l. 10–p. 102 l.1)

D. The Court's Expectations with Respect to the Audit

As part of the Court's oral ruling addressing the PSC's first motion for sanctions, the Court ordered the defendants to take the necessary steps to locate any yet undiscovered material and to report back to the Court ("the audit"). The Court did not expect the "audit" it was ordering to uncover voluminous or broad based materials. Given an expected limited scoped and the already very untimely nature of the disclosures, the Court required completion within mere days. The audit has revealed some gaps in discovery that the Court expected to find. For example, emails such as those of Dr. Clemons' which were not stored in his custodial file and a few BIPI and BII custodians who reported finding some additional documents not previously disclosed. The Court does not now take umbrage with these matters because given the issues that had long plagued this litigation which were discussed at the first sanction hearing, it was anticipated that such matters, hopefully minimal in number, would be uncovered by the court-ordered audit.

***6** There are, however, a growing number of "gaps" in production to which the Court takes considerable exception. The Court has asked repeatedly throughout the many discussions about discovery problems, and at the first sanction hearing, how these problems could be occurring and for such a duration of time. The answer is now clear to the Court. The defendants have taken a too narrow and an incremental approach to its "company-wide" litigation hold.

The Court has been relying on the common

meaning of the words that that the defendants have a company-wide litigation hold on all persons who have custody of any documentation relevant to Pradaxa. The production requests of the plaintiffs are so broad as to cover any possible derivation of means to document someone's thoughts, words and deeds short of attaching electrodes to their scalps and electronically downloading what is contained in their minds. This extreme statement is meant to convey that all of the materials that are discussed in this order were clearly covered by production requests and further anticipated by the Court as subject to the "company-wide" litigation hold.

The Court has examined the defendants' "holds," submitted *in camera*, and does not take umbrage with the language or scope thereof. As it turns out, the problem was in the implementation. For example, the Court learned at the second sanction hearing that the defendants chose to incrementally place holds on certain classes of employees, and have unilaterally chosen not to hold regarding an employee because the company decided he didn't fit the description of "important enough" and wasn't specified by the PSC. Further, while their vendor was given access to one part of a computer drive, it did not have password access to a subpart with relevant material. All of the materials discussed heretofore, should have been produced long, long before now. Some may never be able to be produced.

The defendants have had many conversations with the Court regarding discovery problems. During these conversations, the defendants did not hesitate to voice concerns regarding issues associated with the timing of producing certain documents, data or files. The defendants, however, never sought leave of Court to delay the implementation of the litigation hold on the premise that it was too burdensome—financially or logistically. Therefore, the Court relied on the presumption that the defendants were preserving all relevant documents of every description. It only came to light recently that such was not the case. The Court did not expect that nor was that the subject of specific discussion in the last sanction debate.

III. CASE–SPECIFIC BACKGROUND AND LEGAL AUTHORITY WITH RESPECT TO THE DEFENDANTS' DUTY TO PRESERVE

A. When the Duty to Preserve Arose

1. Relevant Legal Authority

The duty to preserve documents and material that may be relevant to litigation generally arises with the filing of the complaint. *See* *Norman–Nunnery*, 625 F.3d at 428–429. However, The Seventh Circuit has held that the obligation to preserve evidence arises when a party "knew, or should have known, that litigation was imminent." *Trask–Morton v. Motel 6 Operating L.P.*, 534 F.3d 672, 681 (7th Cir.2008).

2. When the Duty to Preserve was Triggered in This Case

In the instant case, as the Court has previously concluded, BIPI's duty to preserve material relevant to this litigation arose in February 2012 when it received a lean letter regarding the first post-launch Pradaxa product liability suit. BII has indicated that it issued a litigation hold shortly thereafter—in April 2012. For purposes of this order, the Court concludes that BII's duty to preserve evidence relevant to this litigation arose—at the latest—in April 2012.

***7** The Court further notes that at least as of June 2012, the defendants were acutely aware that nationwide litigation involving hundreds of cases (if not more) was imminent. On May 31, 2012, Plaintiff Vera Sellers filed a Motion for Transfer of Actions Pursuant to 28 U.S.C. § 1407. *See* MDL No. 2385 (Doc. 1), *In re Pradaxa Prod. Liab. Litig.* ("MDL Motion"). At that time, approximately 30 product liability actions involving the prescription drug Pradaxa were pending in 14 different federal district courts. The MDL Motion stated that at least "500

additional complaints" were expected to be filed in the near future (MDL Motion p. 2). In June 2012, the defendants filed their responsive brief and included the following argument regarding where the growing number of Pradaxa cases should be consolidated:

> Beyond the pending actions, Plaintiff states that "more than 500 additional Complaints will be filed in the near future." Given the nationwide soliciting, the distribution of forthcoming cases would be expected to be spread across the United States. This is, in fact, what has happened. Even after the "wave" of cases were filed in the Southern District of Illinois, followed by the instant MDL request, various plaintiffs filed cases in the Eastern District of Louisiana (including a purported class action), Middle District of Tennessee, Eastern District of Kentucky, Southern District of Florida, Northern District of Ohio, Eastern District of New York, and the District of South Carolina (removed). This distribution reinforces the national scope of the Pradaxa litigation—both in terms of where the cases stand today and where they are likely to be filed.

MDL No. 2385, *In re Pradaxa Prod. Liab. Litig* (Doc. 54 p. 9). Considering the above, there is absolutely no question that the defendants knew nationwide Pradaxa product liability litigation involving hundreds (if not more) cases was imminent. Therefore, the defendants cannot contend, in good faith, as they attempted to do at the sanctions hearing, that they did not understand the size and scope of this litigation until recently. Nor can they contend that their decision to adopt an extremely limited litigation hold was based on an appropriate good faith belief that this litigation would be limited in size.

B. Scope of Duty to Preserve

The general scope of discovery is defined by Fed. Rule Civ. Proc. 26(b)(1) as follows:

> Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense—including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.

"The key phrase in this definition—'relevant to the subject matter involved in the pending action'—has been construed broadly to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case." *Oppenheimer Fund, Inc. v. Sanders* 437 U.S. 340, 351, 98 S.Ct. 2380, 2389 (1978).

The broad scope of discovery outlined in Rule 26 is vital to our system of justice. *See Hickman v. Taylor*, 329 U.S. 495, 507, 67 S.Ct. 385, 392 (U.S.1947) ("Mutual knowledge of all the relevant facts gathered by both parties is essential to proper litigation. To that end, either party may compel the other to disgorge whatever facts he has in his possession."). It was adopted, in part, to restore a sense of fair play and to combat a growing sense of frustration with the often contentious nature of litigation. *See e.g.*, Roscoe Pound, *The Causes of Popular Dissatisfaction with the Administration of Justice, Address Delivered Before the Convention of the American Bar Association* (Aug. 26, 1906), in 35 F.R.D. 241, 273 (1964).

***8** As other district courts in this Circuit have recognized, this vital element of our discovery process "would be a dead letter if a party could avoid [its duty to disclose] by the simple expedient of failing to preserve documents that it does not wish to produce." *Danis v. USN Communications, Inc.*, 2000 WL 1694325, *1 (N.D. Ill. Oct. 20 2000) (Schenkier, M.J.). "Therefore, fundamental to the duty of produc-

tion of information is the threshold duty to preserve documents and other information that may be relevant in a case." *Id.*

Commiserate with Rule 26(b)(1), the scope of the duty to preserve evidence is broad, encompassing any relevant evidence that the non-preserving party knew or reasonably could foresee would be relevant to imminent or pending litigation. *See, e.g., Langley*, 107 F.3d at 514; *Melendez v. Illinois Bell Tel. Co.*, 79 F.3d 661, 671 (7th Cir.1996); *Marrocco v. General Motors Corp.*, 966 F.2d 220, 223–225 (7th Cir.1992). Thus, once the duty to preserve is triggered, the party owes a duty to preserve evidence that may be sought during discovery and should implement a plan to find and preserve relevant evidence. Finally, a party's duty to preserve information is not a passive obligation; it must be discharged actively. See *Marrocco*, 966 F.2d at 224–25.

C. Timeline of Issues Relevant to Duty to Preserve

The Court notes the following with respect to the defendants' preservation obligation in the instant case:

- February 2012—BIPI's duty to preserve is triggered

- April 2012 (at the latest)—BII's duty to preserve is triggered

- June 2012—the defendants know that nationwide litigation involving hundreds (if not more) Pradaxa product liability cases is imminent

- July 13, 2012—The Court and Counsel for BIPI Discuss the Duty to Preserve. Counsel indicates that BIPI has established a litigation hold and represents that, with respect to custodians, the company issues a physical document preservation notice to custodians of relevant evidence

Transcript of July 13, 2012 Status Conference

17 ***THE COURT:*** So one of the things that I was

18 concerned about—and it turns out it wasn't included in

19 your production order—and that is preservation. Do you

20 have a preservation direction issue corporate-wi[d]e? [FN2]

21 ***MR. HUDSON:*** Yes, Your Honor.

22 *THE COURT:* People understand, obviously, this is

23 not your first—presume this is not your first piece of

24 litigation in this corporation.

25 ***MR. HUDSON:*** It's not, and the cases filed here

Page 23 of 33

1 were not the first filed cased, so there were preservation

2 orders in effect before these cases were even filed.

3 ***THE COURT:*** So explain to me essentially how

4 that—without revealing any attorney-client privilege, how

5 does that work and how is it maintained and how is it

6 policed in effect? Briefly. I don't need—

7 ***MR. HUDSON:*** Let me think about how to best explain

8 this. I know the process but I want to be careful about

9 discussing in open court the process the corporation uses

10 for this, because there are attorneys involved, but there is

11 a physical document preservation notice that is issued to

12 potential custodians of relevant evidence. There's a

13 process by which the custodians confirm acknowledgment of

14 the obligation to comply with the litigation hold, and that

15 is monitored and followed up on.

16 And I think—Your Honor, does that adequately

17 answer your question or would you like me to go into more

18 detail there?

19 *THE COURT:* No, that's fine. And in general, there

***9** 20 are officers, coordinators, employees who are charged with

21 overseeing the preservation?

22 *MR. HUDSON:* Individuals within the legal

23 department, and there are contact points identified on the

24 preservation notice as well, as far as who the people are

25 involved in that process. So the people charged with the

Page 24 of 33

1 preservation obligation receive the document preservation

2 notice, actually know who—in addition to the person who's

3 issued the letter from the legal department, but the person

4 they can go to with questions, yes.

(Doc. 57 p. 22 l.17–p. 24 l.3)

• **November 5, 2012**—Counsel for BII confirms that BII is aware of the Court's preservation order (Doc. 69 p. 11 l.14–17) ("As I told the Court in chambers, BII is aware of the preservation obligations, and document preservation notices went out prior to the cases being transferred to this MDL.").

FN2. The Court, based on independent recollection, agrees with plaintiffs' assertion that the transcript contains a transcription error. The transcript reads “wise” but should read “wide.” Further, as the Court noted during oral argument, it finds no difference in the terms.

IV. POTENTIALLY SANCTIONABLE CONDUCT PRESENTLY IN ISSUE

A. Thorsten Lehr

1. Background

Professor Thorsten Lehr is a pharmacometrician formerly employed by BII (Doc. 311 p. 9). While working for BII, Prof. Lehr was a high-level scientist that worked on Pradaxa and published articles on Pradaxa as a lead author (Doc. 302 p. 5). Prof. Lehr was responsible for quantitative analysis relating to the interaction between Dabigatran and specific patient populations (Doc. 302–5 p. 5). Prof. Lehr left employ at BI at the end of September 2012—well after the defendants were under a duty to preserve evidence relevant to this litigation (Doc. 302–4 p. 6; Doc 302–5 p. 5). Dr. Lehr is currently employed by Saarland University (Doc. 302–5 p. 5). There is a cooperation agreement between BII and Saarland University under which Prof. Lehr continues to have access to certain Pradaxa clinical trial data (Doc. 302–5 p. 5).

According to the PSC, BII never disclosed Prof. Lehr in any answers to the PSC's interrogatories. Further, Prof. Lehr was not on the list of custodians with relevant knowledge provided by BII. *Id.*

The PSC did not learn of Prof. Lehr's relevance to this litigation until September 25, 2013 when Lehr was identified during the deposition of one of the defendants' employees, Martina Brueckman (Doc. 317–1 p.6). That same day, the PSC requested Prof. Lehr's custodial file be produced by October 7, 2013 (Doc. 317–1). BII did not respond to the request for production of Prof. Lehr's custodial file for two weeks and at that time indicated that it would need 45 days to produce his custodial file (invoking a case management order previously adopted by the Court) (Doc. 317–1).

On October 25, 2013, in a letter to the Court, BII stated that Prof. Lehr “was not subject to a litigation hold when he left BII because he had not been identified as a custodian” (Doc. 302–5 p. 5). On November 4, 2013, BII again informed the Court that Prof. Lehr was not subject to a litigation hold when he left the company because he had not been identified as a custodian (Doc. 302–4 p. 6), On November 7, 2013, counsel for BII (Beth S. Rose) provided an affidavit with additional information pertaining to Prof. Lehr (Doc. 302–6). The affidavit provides, in relevant part, as follows:

> ***10** Contemporaneous with this Affidavit BII is making the production of responsive e-mails from Thorsten Lehr. Thorsten Lehr is a former BII employee who formally left the company at the end of September 2012. At the time he left, Prof. Lehr was not identified as a custodian and, therefore, was not subject to the document preservation notice. We have confirmed with Prof. Lehr that when he left the company, he did not take his workstation or any other documents with him. Prof. Lehr's workstation, user share, and paper documents are not available to be collected. The only part of Prof. Lehr's custodial file available for collection is his e-mails.

(Doc. 302–6 ¶ 2). In other words, with the exception of Prof. Lehr's emails, BII failed to preserve Prof. Lehr's custodial file at a time when it was under a duty to do so.

BII has stated that they chose not to preserve Dr.

Lehr's custodial file because, at the time of his departure in September 2012, he had not been identified as a custodian. This statement lends itself to one of two interpretations. Either BII is asserting that it did not realize that Prof. Lehr was a custodian with potentially relevant information and therefore failed to preserve his custodial file when he left the company; or BII is asserting that because the PSC had not yet requested Dr. Lehr's custodial file, it had no duty to preserve Dr. Lehr's custodial file (even if it contained information relevant to this litigation). Both interpretations are problematic for BII.

2. BII Cannot Believably Contend it Did Not Recognize Prof. Lehr as a Custodian with Potentially Relevant Information

BII cannot believably contend it did not know Prof. Lehr's custodial file contained information relevant to this litigation. Prof. Lehr was unquestionably a high-level scientist actively involved in working on Pradaxa. For instance, in an email dated May 31, 2012, Dr. Yasser Khder (employed by BII) introduces "Dr. Thorsten Lehr" to his "colleagues" as "our company expert for dabigatran" (Doc. 317–1 p. 16). He goes on to state that Prof. Lehr "did all the M & S for the [REDACTED BY THE COURT] program (Doc. 317–1 p. 16). Dr. Lehr will get in contact with you to further discuss the different aspects to this request" (Doc. 317–1 p. 16).

The PSC has also learned that Prof. Lehr co-authored at least 10 Dabigatran (Pradaxa) articles published between September 2011 and September 2013 (Doc. 317–1 pp. 9–14). Further, although Prof. Lehr is no longer employed by BII, he continues to work with BII scientists on future Pradaxa publications (Doc. 317–1 p. 14).

Even more telling, is a group of company emails exchanged in 2011 and 2012 reflecting an internal debate over whether a scientific paper being drafted by Prof. Lehr (the "exposure paper") should include Prof. Lehr's conclusions regarding Pradaxa's therapeutic range.[FN3] In the exposure paper, Prof. Lehr (and his co-authors) concluded, in the early versions of the paper, that both safety and efficacy of dabigatran are related to plasma concentrations and conclude that there is a therapeutic range for Pradaxa and further specify what that range is. (Doc. 317–1 p. 20).

> FN3. Notably, in an email dated October 31, 2012, addressed to Dr. Jeffrey Friedman, Dr. Andreas Clemens (BIPI employee) refers to Dr. Lehr as the "father" of the exposure paper (Doc. 317–1 p. 17).

These emails reveal Dr. Lehr's desire to publish a paper that included a therapeutic range for Pradaxa was highly controversial. An email from Dr. Andreas Clemens, dated December 19, 2011, demonstrates the discussion and disagreement flowing through the company regarding Dr. Lehr's conclusions (Doc. 317–1 p. 23). As does a July 30, 2012 email from Stuart Connolly (Doc. 317–1 p. 29). Ultimately, an email from Dr. Jeffrey Friedman, dated October 23, 2012, seems to require a revised version of the exposure paper without inclusion of the therapeutic levels suggested by Prof. Lehr (Doc. 317–1 p. 31). An email from Dr. Clemens to Prof. Lehr, dated October 24, 2012, confirms that (Doc. 317–1 p. 33).

***11** The following email describes Prof. Lehr's position on the matter at the end of October, 2012.

October 31, 2012 email from Dr. Andreas Clemens

> Thorsten wants to tailor the message according our ideas. I see value in this manuscript especially with regard to a manuscript which will in the next step focus on lab levels (aPTT) to give the physicians an understanding what they have to expect in specific situations regarding aPTT. The world is crying for this information—but the tricky part is that we have to tailor the messages smart. Thorsten wants to do that.
> (Doc. 317–1 p. 17).

Eventually, another scientist, Paul Reilly, was tasked with revising the exposure paper. The following email from Paul Reilly further demonstrates the internal debate over inclusion of an optimal therapeutic range in the exposure paper:

> I have been facing heavy resistance internally on this paper about the concept of a therapeutic range, at least stating it outright. Perhaps you can help me with solving this dilemma. I am working on a revision to deal with this and I will come back to you with it. I think they just don't want the message that one range fits all, it's patient specific.
>
> (Doc. 317–1 p. 28).

The emails also reveal the importance of keeping the debated issue confidential. Dr. Clemens October 24, 2012 email to Prof. Lehr (above) closes with a statement written in German, roughly translated as follows:

> I think—"the banana is still shuttered". Please treat this confidential because Jeff currently interacts with Paul Reilly directly—and I do not know if they know this is actually on file.
>
> (Doc. 317–1 p. 33). Prof. Lehr subsequently responded to Dr. Clemens' request for confidentiality as follows:
>
> I will keep it absolutely confidential! I'm personally very disappointed about the exposure-response manuscript. I have put a LOT of effort and time into the analysis. But I don't like the way how the manuscript is written and the message conveyed. I'm working again on a revision of the document and I hope that Paul will consider them. It is the last time, that I agree to put people as first author who were not involved in data analysis. Let's try to get this manuscript in a shape that everybody is happy. Maybe we need a TC (Jeff, Paul, Andreas, Thorsten) to discuss open issues.
>
> (Doc. 317–1 p. 34).

In addition, the emails exchanged during this time period demonstrate that the exposure paper and Dr. Lehr's controversial conclusions regarding an optimal dosing range for Pradaxa were being considered and discussed in the highest levels of the company and with the defendants' legal team. For example, consider the following emails:

December 19, 2011 email from Dr. Janet Schnee to Dr. Andreas Clemens

> I noticed this email only this evening, but have now forwarded [Dr. Lehr's draft exposure paper] to the U.S. product lawyer for an opinion.
> (Doc. 317–1 p. 24)

June 4, 2012 email from Dr. Paul Reilly

> Exposure response is definitely on the OC radar and I have been heavily pressed to revise and submit the manuscript. It has been "on hold" for almost 6 months. I had to wait several weeks for some analyses from Thorsten, at his request.
> ***12** (Doc. 317–1 p. 25)

July 16, 2012 email from Dr. Lehr to Paul Reilly

> I met Jeff last Thursday. We discussed the ER [exposure paper] analysis together with management. As management liked it (and also Jeff seemed to like it), I believe we have some tailwind. Maybe you can meet with Jeff and see how to move forward.
> (Doc. 317–1 p. 26)

Considering the material pertaining to Prof. Lehr, including the email excerpts noted above and those not excerpted for confidentiality purposes but which the Court was able to read in the motions filed

under seal, it is evident that Dr. Lehr was a prominent scientist at BII that played a vital role in researching Pradaxa. The defendants' management, legal team, and other top-scientists were familiar with Prof. Lehr's work and communicated with him regarding the same. The Court is stunned that Prof. Lehr was not identified by the defendants as a custodian with potentially relevant knowledge about Pradaxa. Further, given the above, it is evident that the defendants knew that Prof. Lehr's custodial file contained information relevant to this litigation in September 2012 when Prof. Lehr left his employ with BII. The emails also may lead a reasonable person to infer a motive for the defendant to abstain from placing a litigation hold on his materials, including the early versions of the exposure paper. The entire debate is relevant, or at least conceivably relevant, to this litigation and without question any documents, no matter who generated them, should have been the object of the litigation hold.

3. The Duty to Preserve is not Defined by What has or has not Been Requested by Opposing Counsel

The second possible interpretation of BII's statement regarding why it chose not to preserve Dr. Lehr's custodial file is that BII is blaming the PSC for failing to identify Dr. Lehr as a custodian. In other words, a party only has a duty to preserve relevant evidence that has actually been requested by the opposing party. This position is nonsense. The very purpose of the duty to preserve, is to protect potentially relevant material so it is available for production when and if the opposing party requests that material. Furthermore, the defendant, not the plaintiff, is in the best position to identify persons such as Dr. Lehr.

4. Final Points Regarding the Defendants' Supplemental Response

During oral argument, the PSC showed the Court draft version number 5 of the exposure paper. The PSC raised questions regarding whether draft versions 1–4 had been destroyed. In their supplemental response, the defendants contend that their productions have included seven earlier distinct drafts of the exposure paper (presumably from sources other than Prof. Lehr's custodial file), dating back to January 2011 (Doc. 317 p. 2). This argument misses the point. The defendants do not get to pick and choose which evidence they want to produce from which sources. At issue here are the missing documents and material contained in Dr. Lehr's custodial file. The question is, of the draft versions stored on Dr. Lehr's work stations, what was lost when the defendants failed to preserve Dr. Lehr's custodial file.

***13** The defendants also argue that because their preservation obligation only attached in February of 2012, they were under no duty to produce documents created prior to February of 2012 (Doc. 317 p. 2). This contention distorts the nature of the duty to preserve. The fact that the defendants preservation obligation did not attach until February of 2012 (or, at the latest, April of 2012 for BII), does not mean that the defendants are entitled to destroy documents created prior to that date. It means that as of February 2012, the defendants have a duty to preserve any documents in the defendants' control—even those created before February 2012—that are potentially relevant to this litigation and destruction occurring after February 2012 is a violation of that duty.

Finally, the defendants contend that because they have produced discovery from other sources that reveals the internal dispute over the exposure paper and over issues relating to therapeutic range, the failure to preserve Prof. Lehr's custodial file must be innocent (Doc. 317 pp. 3–4).[FN4] In light of all the other discovery abuses that have been discussed herein, this argument does not win the day. One does not know what annotations are or were contained on the personal versions of Dr. Lehr or what statements he made in his “share room” space about the controversy that was brewing. Plaintiffs are entitled to discovery on such matters for interrogation or cross exami-

nation purposes.

> FN4. This position was also asserted during oral argument when counsel for BIPI argued, in essence, that if this was a cover-up it was the worst cover-up in the world.

B. Inadequate Litigation Hold for Pradaxa Sales Representatives, MSLs and CSCs

1. Background

The Court will now address issues related to the litigation hold as it was applied (or not applied) to the defendants' Sales Representatives, Clinical Science Consultants (CSCs) and Medical Science Liaisons (MSLs). First, however, the Court will provide some background with regard to CSCs and MSLs.

CSCs are specialized sales representatives.[FN5] In November 2011, CSCs began delivering unbranded disease state messages to health care providers concerning atrial fibrillation ("A-fib") (Pradaxa is used to reduce the risk of stroke and blood clots in people with A-fib not caused by a heart valve problem) (Doc. 271 p. 8). Purportedly, CSCs met with physicians to discuss A-fib without reference to Pradaxa (Doc. 271 p. 8). According to the defendants, the CSCs received Pradaxa-specific training in September 2012 to address physician questions they were receiving from physicians related to Pradaxa. Notably, the existence of the CSC sales force was never disclosed by the defendants even though this information was specifically requested by the PSC in prior discovery and in the Defendant Fact Sheet ("DFS") (Doc. 266 p. 18–19; Doc. 302–8 § II.C). Instead, the PSC discovered the existence of CSCs only when they noticed the word "CSC" in other documents the defendants had produced (Doc. 266 p. 19). The PSC began asking about the CSCs by title in July 2013 (Doc. 266 p. 19). The defendants repeatedly told the PSC that all of the CSC physician call information was contained in the VISTA database and had already been produced (Doc. 266 p. 19). The PSC was suspicious of this answer and continued to press the issue. Only after another five conversations with the defendants was it learned that there was in fact a separate field within VISTA that contained the CSC data and that this field had not been disclosed to the PSC and had not been produced (Doc. 266 p. 20). Defendants insisted that this was an unintentional oversight and on September 10, 2013 provided the PSC with the missing information (Doc. 271 p. 8).[FN6]

> FN5. In the PSC's initial motion for sanctions, they describe CSCs as follows:
>
> > [A CSC] is a part of the promotional arm of BIPI and specifically Pradaxa. CSCs are individuals with some level of advanced education or certification such as PharmD. They serve a nuanced purpose of delivering an "unbranded" message to physicians, allowing them to say things that a sales representative could not say, such as discussing a-fib rather than non-valvular a-fib, and discussing Warfarin in general terms and not just in relation to comparison studies. The documented purpose of the CSC was to 'disrupt' physicians' confidence in Warfarin. The CSCs originally did not discuss a particular product to treat the disease, but in theory were trying to raise disease awareness—however they never raised awareness of a disease Defendants did not have a product to treat. In fact, originally BIPI had 'guardrails' to prevent a doctor from being detailed about a product within 24 hours of a call by a CSC because they wanted to avoid the appearance of 'off-label' promotion. In 2012, however, CSCs began to educate the doctors on the branded product—here Pradaxa—at the same visit they raised awareness to a disease.

(Doc. 266 p. 19).

FN6. In addition, the defendants noted that they could not possibly have intended to hide the CSC data considering they produced documents from other sources which referenced CSCs. They also noted that the omitted data was only a small percent of the total data produced in the VISTA data base. Similar arguments have been raised in response to the PSCs current motion for sanctions.

***14** MSLs are another separate specialized group within BIPI. The defendants describe MSLs as "individuals with medical and scientific backgrounds whose role is to interact with health care providers who are deemed to be scientific experts and key opinion leaders" (Doc. 271 p. 9). According to the PSC, MSLs were "responsible for making direct contact with a physician under the auspices of having a scientific conversation about a-fib, Warfarin and other subjects that could not be discussed as part of the direct promotion of Pradaxa" (Doc. 266 p. 20). Information about MSL visits with physicians is contained in what is known as the BOLD database. The existence of BOLD was not disclosed to the PSC in discovery or as part of the 30(b)(6) deposition process. Instead, the existence of MSLs and BOLD was disclosed to the PSC only in relation to the PSC uncovering the CSC issue and only when the PSC asked the defendants if there were any other forces that called on physicians (Doc. 266 p. 21). The defendants "[did] not dispute that the BOLD database and relevant MSLs should have been identified and produced to Plaintiffs earlier in this litigation (Doc. 271 p. 10). They insisted, however, that this failing was another innocent inadvertent mistake.

2. Inadequate Litigation Hold

In recent weeks, it has come to light that the defendants' litigation hold, as it relates to Pradaxa sales representatives, MSLs, and CSCs, has been grossly inadequate for a litigation of this scope and size. On November 4, 2013, the defendants informed the Court and the PSC that they had been "addressing questions recently raised at sales representative depositions that the volume of email produced for certain witnesses was smaller than expected," (Doc. 302–4 p. 2). The PSC had also raised concerns that individual sales representatives custodial files did not seem to go back sufficiently far in time (Doc. 311 p. 12). In reviewing these questions, the defendants decided to "examine the dates that the sales reps/CSCs/MSLs requested for the deposition became subject to the litigation hold" (Doc. 302–4 p. 2). This examination revealed following:

• When the defendants first instigated a litigation hold in February 2012, they only intended to apply the hold to the specific sales representatives who detailed specific plaintiff's physicians. It takes time, however, to identify each plaintiff's prescribing physician and the corresponding sales representative(s). Rather than taking steps (such as placing all Pradaxa sales representatives on a litigation hold) to preserve the relevant material while these specific sales representatives were identified, the defendants did nothing.

• It was not until September 26, 2012, at which point 127 cases were on file, that the defendants decided to "expand" the then non-existent litigation hold for Pradaxa sales representatives (Doc. 311–15 p. 2; Doc. 311 p. 13). Even then, however, the litigation hold was only applied to those Pradaxa sales representatives *currently* detailing Pradaxa (Doc. 311 p. 13).

• In March 2013, with 262 cases filed, the defendants finally decided to extend the litigation hold to all sales representatives who had ever detailed Pradaxa (Doc. 311 p. 13).

• The Clinical Science Consultants (CSCs) and Medical Science Liaisons (MSLs) who detailed Pradaxa were not included in the litigation hold until August 2013 (Doc. 311 p. 13). However, the only CSCs and MSLs included in *this* hold were the CSCs and MSLs who detailed the treating physicians in the bellwether cases.

• All CSCs and MSLs who detailed Pradaxa were not placed on litigation hold until sometime after August 2013 (the defendants responsive brief simply states that they "subsequently" added "the remaining CSCs and MSLs"—the Court suspects that "subsequently" means just before the defendants filed their responsive brief) (Doc. 311 p. 13).

The litigation hold described by the defendants is wholly inadequate in light of the size and scope of this litigation. The defendants were under a duty to preserve information that they knew or reasonably could foresee would be relevant to imminent or pending litigation. In the instant case, the duty to preserve arose in February 2012 for BIPI and in April 2012 (at the latest) for BII. Once the duty to preserve was triggered, the defendants owed a duty to preserve evidence that may be sought during discovery and should have implemented an adequate plan to find and preserve relevant evidence.

***15** The defendants argue that the proportionality requirement of Rule 26 allowed them to implement an extremely narrow litigation hold.[FN7] They contend it would have been unreasonable to require them to place, for example, all Pradaxa sales representatives on a litigation hold. That might be true if this was a regional case involving only a few plaintiffs with no indication of the litigation expanding into nationwide litigation. That, however, is not the scenario we are faced with. As discussed above, as of June 2012, the defendants were aware that nationwide Pradaxa product liability litigation involving hundreds of cases (if not more) was imminent. They argued this very fact before the MDL panel in June 2012. The Court is frankly amazed that the defendants could raise such an argument and now argue, before this Court, that they did not fully understand the broad scope of this litigation or the need to expand their litigation hold to *all* Pradaxa sales representatives, CSCs, and MSLs until March 2013 (sales representatives) and sometime after August 2013 (CSCs and MSLs) (*See* Doc. 311 pp. 12–13; Doc. 311 p. 13 ("Defendants expanded the scope of their sales representative preservation efforts as the litigation expanded in size"). Furthermore, there is nothing in any case management order nor can defendants point to any statement of the Court that can be interpreted as suggesting such a tailored litigation hold was acceptable. Defendants did not receive from the Court a protection order tailoring the litigation hold or managing in increments classes of employees on some timeline or on some case specific landmark when the litigation hold would kick in. There have been no regionally based markers designed to apply the litigation hold to certain sales or consulting staff based on case filings. The defendants' efforts to suggest they and they alone decided to implement such a proportionality test to the litigation hold smacks of a post-debacle argument in desperation to salvage a failed strategy regarding production evasion.

> FN7. This argument is raised in the defendants' response, supplemental response and was raised by the defendants at oral argument.

The defendants also argue that because they have produced certain databases and/or document repositories that warehouse relevant sales representative, CSC and MSL material any failings with regard to these employees' custodial files is of little or no consequence (Doc. 311 p. 10). For instance, the defendants note that they have produced approximately 45,000 pages of documents from the TEMPO database, which contains the documents used to train

sales representatives about Pradaxa and the promotional pieces that the sales force is approved to use in detailing health care providers on Pradaxa, along with earlier drafts of these materials (Doc. 311 p. 10). The defendants note sales representatives have consistently testified they are not permitted to use and do not use material outside of the TEMPO database when detailing physicians (i.e. they only used the approved TEMPO material) (Doc. 311 p. 10). Obviously, the defendants contend, the PSC doesn't really need material from the sales representatives' custodial files, because the only material sales representatives used can be found in the TEMPO database.

This argument is ridiculous. The PSC is entitled to the requested material so they can determine for themselves whether the sales representatives only used approved material from the TEMPO database. In addition, they are entitled to review the files for other relevant information to utilize as a basis for cross examination. An example leaps to the fore, what if a sales representative has in his notes that he made some fraudulent representation about Pradaxa to a physician. Further, what if the rep said "as directed by so and so, I told Dr. X this and that" which is known by all to be patently false? Obviously, the training materials alone are not relevant and clearly the Court does not suggest that its hypothetical is accurate. However, if it were to prove true, the defendants' cannot deny such material is both relevant and discoverable.

C. The G Drive

The G Drive and T Drive are shared network drives made available to certain of defendants' employees. Defendants Letter to Court, October 7, 2013. According to the defendants, employees generally use these drives to store departmental data. *Id.* Within BIPI, this drive is known as the G Drive; within BII, it is known as the T Drive. Although potentially serious production issues have been identified with both the G Drive and the T Drive, only the production issues associated with the G Drive are presently before the Court.[FN8]

> FN8. The defendants have reported similar issues with the T Drive production and have informed the Court and the PSC that they now realize that "large portions" of the T Drive were not included in the original T Drive collection (Doc. 311 p. 18).

The G Drive is not a single unified electronic storage area. It consists of over 1.8 million folders (Doc. 311 p. 17). Employees are granted access to the folders depending on the needs of their job (Doc. 311 p. 17). If an employee does not have access to a folder on the G Drive, it will not appear at all when he or she logs into the G Drive (Doc. 311 p. 17).

***16** Pursuant to Case Management Order Number 17, the G Drive was scheduled to be produced on or before January 30, 2013 (Doc. 78 ¶ 14). In accord with the certification requirement imposed on the defendants as a result of earlier discovery violations (CMO 38 Doc. 231), the defendants provided an affidavit of completion of document production in relation to the G Drive on August 7, 2013 (Doc. 317–14 p. 43). The original G Drive production included approximately 3.5 million pages (Doc. 311 p. 18).

Shortly before the Court held a hearing on September 18, 2013 (to address the PSC's first motion for sanctions), the defendants alerted the PSC to potential problems with the G Drive production (October 7, 2013 Letter to the Court). The defendants indicated that approximately 500,000 documents/files (excluding attachments) from four out of the five G Drive directories were missed and, as a result, were not produced to the PSC (October 7, 2013 Letter to the Court). The defendants further indicated that the number of missed documents/files was expected to increase slightly when the fifth directory was searched (October 7, 2013 Letter to the Court).

Ultimately, the defendants determined that the documents/files were missed because the defendants' IT department failed to provide the third party vendor conducting the G Drive collection proper access to the G Drive (Doc. 311 pp. 17–18). More specifically, the IT department was tasked with providing the third party vendor with logins that would give the third party vendor full access to all folders in the G Drive (Doc. 311 p. 17). The IT department, however, failed to do this (Doc. 311 p. 17). Instead, the IT department gave the vendor "default" logins of the sort typically granted to new employees (Doc. 311 p. 17). These default logins did not have access to all G Drive folders, meaning the vendor was not aware of the existence of some of the folders and did not collect files from them (Doc. 311 p. 18). The defendants eventually produced the missing documents. That supplemental production contained approximately 400,000 pages. This sort of "mistake" early in this litigation would have been looked upon by the Court as just that, but as the rationale of this order makes clear, the reasonable inferences to be drawn from the actions of the defendant at this point in time are that such maneuverers are by design.

The PSC contends that the production indicates that there are numerous new G Drive storage areas that should have been revealed during 30(b)(6) depositions. It further contends that the late production has resulted in prejudice in that they do not yet know what is in it, it was produced in a disorganized manner, and they do not know who uses the new storage areas or what they are used for. The defendants contend that the production was not disorganized and complied with CMO 3 in all respects (with the exception of an error with a meta data field that has since been corrected) (Doc. 311 p. 18). The defendants further contend that no relevant documents from the G Drive have been lost because the G Drive does not have an auto delete function (Doc. 311 p. 18).

D. Text Messages

On June 28, 2012, before creation of the MDL, the PSC specifically requested that BIPI produce text messages (Doc. 302–9). The PSC made a similar request to BII on October 22, 2012 (Doc. 302–10). The defendants have admitted that the PSC did in fact request texts (Doc. 302–4 ("[t]exts were requested in discovery by both parties, and produced by neither, so far as we can tell."; Doc. 311 p. 14 (admitting that the PSC's document requests "included text messages in their boilerplate definition of 'document' "). Amazingly, the defendants' hold applicable to sales representatives, CSCs and MSLs did not expressly extend to text messages until October 18, 2013 or later (Doc. 302 p. 7). The defendants first alerted the Court and the PSC to the issue in a footnote in a letter dated October 25, 2013 (Doc. 302–5 p. 2 n.3). In the footnote, the defendants contend that they did not realize until mid-October that some employees had business related text messages on their cell/smart phones (Doc. 302–5 p. 2 n.3). The PSC (and the Court) question the plausibility of this claim considering the defendants have produced a document showing that the defendants directed their sales force to use texts to communicate with their supervisors, district managers, and others (Doc. 302–2). Further, the deposition testimony of employee Emily Baier raises further questions on this issue.[FN9]

FN9. During oral argument, the PSC played Ms. Baier's testimony. Among other things, Ms. Baier stated as follows: (1) she utilized a company issued phone; (2) she utilized text messaging for work-related communications for years; (3) she was alerted to a litigation hold in September 2012 but she does not recall being asked to retain text messages; and (4) she received an email from counsel about one week prior to her deposition regarding the need to retain text messages.

***17** The defendants contend that they have "consistently included a broad definition of 'document' in the document preservation notices sent to potential custodians and—while the notices do not explicitly

state 'text messages'—they do tell custodians to preserve all relevant documents in any form, particularly specifying that this includes electronic communications stored on hand held devices" (Doc. 311 p. 14). The defendants further contend that the late discovery of the existence of business related text messages on certain employees' phones is the fault of their employees (Doc. 311 p. 15 "Until October of 2013, however, BI custodians did not identify text messages among their responsive documents ..."). The Court does not accept this explanation. As noted above, the duty to preserve is not a passive obligation; it must be discharged actively. The defendants had a duty to ensure that their employees understood that text messages were included in the litigation hold. The defendants' own documentation directs employees to utilize text messaging as a form of business related communication. Questions should have been raised by the defendants prior to October 2013 when none of their employees were producing text messages.

Yet another, perhaps more egregious, example of the defendants failure to properly exercise a litigation hold with respect to employee text messages, is the revelation that the defendants failed to intervene in the automated deletion of employee text messages on company issued phones. The PSC has discovered that many employees utilized company issued cell phones. Apparently, the company issued cell phones were auto-programmed (by the defendants) to delete employee text messages.[FN10] The defendants' failure to intervene in this automatic process places them outside of the "safe-harbor" provision provided for in Federal Rule 37(e) and subjects them to sanctions for the loss of any electronically stored information resulting from that failure. *See* Committee Comments to Fed. R. Civ. Proc. 37(f)(now 37(e):

> Rule 37(f) applies to information lost due to the routine operation of an information system only if the operation was in good faith. Good faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation. A preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order in the case. The good faith requirement of Rule 37(f) means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve. When a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a "litigation hold." Among the factors that bear on a party's good faith in the routine operation of an information system are the steps the party took to comply with a court order in the case or party agreement requiring preservation of specific electronically stored information.
>
> FN10. The auto-delete function on company issued cell phones and the defendants' failure to halt the auto-delete function once a litigation hold was in place was revealed during the deposition of Emily Baier on November 14, 2013.

In their supplemental response, the defendants argue that while sanctions might be appropriate for failure to turn off an auto-delete function in relation to email communications the same conduct with respect to text messages is not sanctionable (Doc. 317 p. 5). The basis for their argument seems to be that text messages are a less prominent form of communication and that the production of text messages is too burdensome (Doc. 317 p. 5). As to the former, text messages are electronically stored information, it does not matter that text messaging is a less prominent form of communication. Further, in the instant case, employees used text messaging—to some extent—for business related communication and text

messages were expressly requested by the PSC. There is no question the defendants owed a duty to preserve this material. As to the latter, the Court has already addressed the issue of burden. If the defendants felt the PSC's request for text messages was overly burdensome they should have filed the appropriate motions with the Court. The defendants cannot simply make a unilateral decision regarding the burden of a particular discovery request and then allow the information that is the subject of the discovery request to be destroyed.

***18** In their supplemental brief, the defendants also note the following: (1) although Ms. Baier utilized text messaging for work related communications, she also testified that these text messages were non-substantive and (2) the company has a policy prohibiting substantive text messaging with physicians (Doc. 317 p. 6). As a result, the defendants argue, their failure to preserve text messages is harmless (Doc. 317 p. 6). Once again, the defendants do not get to choose which evidence they want to produce and from which sources. The PSC is not required to simply accept as true the assumption that all employees followed the "no substantive communications with physicians" policy. Nor is it required to accept as true a deponent's claim about the content of her electronic communications. It is certainly common knowledge that texting has become the preferred means of communication. The PSC is entitled to the discovery requested for, among other things, the purpose of impeaching the above claims.

Finally, the defendants argue that they do not believe they are required to produce text messages anyway (Doc. 311 p. 15). This is a classic example of conduct on behalf of the defendants that has become all too familiar in this litigation. The PSC refers to the practice as "better to beg forgiveness than ask permission." If the defendants felt they did not have an obligation to produce the text messages requested by the PSC, they should have responded with a specific objection to the request or otherwise sought relief from the Court. *See* Fed. R. Civ. Proc. 34(b) and 26(c).

The defendants raised the issue that some employees use their personal cell phones while on business and utilize the texting feature of those phones for business purposes yet balk at the request of litigation lawyers to examine these personal phones. The litigation hold and the requirement to produce relevant text messages, without question, applies to that space on employees cell phones dedicated to the business which is relevant to this litigation. Any employee who refuses to allow the auto delete feature for text messages turned off or to turn over his or her phone for the examination of the relevant space on that phone will be subject to a show cause order of this Court to appear personally in order to demonstrate why he or she should not be held in contempt of Court, subject to any remedy available to the Court for such contempt.

VI. FINDINGS AND CONCLUSIONS

A. Findings as to Bad Faith and Otherwise Culpable Conduct

The Court finds the actions and omissions of the defendants, BIPI and BII, to be in bad faith. The defendants argue that their failure to produce the many thousands of documents they are now producing, and their inability to produce other documents at all, are the result of a good faith measured approach to the production of millions of documents over a fairly short period of time. They contend their failure to designate certain employees as subject to a hold is part of a reasonable hold strategy based on a measured and proportioned approach to cost benefit analysis dependant on scope of litigation. They base their failure to include one scientist in the litigation hold on a failure of their opponents to designate him and their own determination that he singularly was not important enough in light of including his coworkers whose custodial materials were being provided.

As the Court mentioned hereinbefore, the ques-

tion the Court has been asking over and over again has been answered. How can these problems keep happening? One of the problems to which the Court has been referring was that the defendants kept coming up with materials in an untimely manner. Materials were being turned over months and months late—often on the eve of a deposition. It is clear to the Court that the defendants have been pursuing a policy of turning over relevant material, or withholding relevant material, on their schedule and not the Court's. In doing so, they have violated the Court's case management orders. They have made misrepresentations to the Court in open court and in chambers. The defendants have caused the Court to believe that each defendant had a litigation hold, company-wide, on all relevant personnel and all relevant documentation and data (in their broadest definitions) at all relevant times.

***19** The Court finds that BII has specifically not applied the hold to Dr. Lehr and now failed to produce certain of his "files." To fail to do so was in violation of the Court's case management orders and in bad faith.

The Court finds both defendants failed to ensure that the auto delete feature of their employee cell phones, company owned and personal, was disengaged for the purpose of preserving text messages and, as such, this allowed countless records to be destroyed. One can only speculate about the relevance or lack thereof and what aspect of plaintiffs' case was harmed thereby. The Court finds this action to be in violation of its case management orders to produce relevant material by a date certain and in bad faith.

The Court finds the defendants failure to place a litigation hold on Sales Representatives, Clinical Science Consultants and Medical Science Liaisons at the earliest date and across the board of all such persons having any involvement with Pradaxa, and thereafter producing the relevant materials in a timely manner, in violation of the Court's case management orders, and in bad faith.

The Court finds that the failure to provide the vendor hired to provide the plaintiffs with discoverable material from the G drive with all relevant materials to be in violation of the Court's case management orders and in bad faith.

B. Sanctions Imposed

1. Professor Thorstein Lehr

The Court directs BII to produce all complete "files" [FN11] of Professor Lehr within 7 days. If that proves impossible because they have been destroyed due to the fact that he was not subject to the litigation hold, defendant shall so certify to the Court. Once the Court, knows for certain what defendant's response to this order is in this regard, a further order will issue, allowing more time with possible conditions, or an order assessing sanctions pursuant to Rule 37 or the Court's inherent authority, if appropriate.

> FN11. The Court will not endeavor to break down this word here or throughout this order any more specifically or technically than this, suffice it say defendant(s) shall interpret this in the broadest sense possible to mean all paper and electronic documents and data of every description. Further, complete is interpreted to mean going back in time from the inception of the keeping of any such relevant documentation or data by the individual.

2. Inadequate Litigation Hold as to Sales Representatives, CSCs and MSLs

The defendants, BIPI and BII, are ordered to produce the complete files for those sales representatives, CSCs and MSLs that have been requested by the PSC within 14 days. If the defendants are unable to comply with this order, they shall so advise the Court and advise if more time is needed and the rea-

son or if certain files are not available and the reason. The Court will then issue an order allowing more time with possible conditions, or an order assessing sanctions pursuant Rule 37 or the Court's inherent authority, if appropriate.

3. Failure to Preserve Text Messages

The defendants, BIPI and BII, are ordered to produce any text messages not otherwise covered by the order directed in number 2 immediately above that have been requested by the PSC within 14 days. If the defendants are unable to comply with this order, they shall so advise the Court and advise if more time is needed and the reason or if certain files are not available and the reason. The Court will then issue an order allowing more time with possible conditions, or an order assessing sanctions pursuant Rule 37 or the Court's inherent authority, if appropriate.

4. G Drive

***20** The defendant, BIPI, is ordered to produce any relevant portions of the G drive that have been requested by the PSC within 30 days. If the defendant is unable to comply with this order, it shall so advise the Court and advise if more time is needed and the reason or if certain files are not available and the reason. The Court will then issue an order allowing more time with possible conditions, or an order assessing sanctions pursuant Rule 37 or the Court's inherent authority, if appropriate.

5. Financial Sanctions

The PSC requested a number of financial sanctions as a result of the defendants' transgressions. It asked for reimbursement for its fees and costs in pursuing the issue of the defendants' violations. The defendants agree they should be held accountable for that and the Court so orders and directs the PSC to submit an itemization with an affidavit.

The PSC requested that the Court revisit the issue raised by it through motion that the employee depositions scheduled or to be scheduled in Europe be scheduled in a place convenient to the PSC and defendants' United States counsel. This is a financial issue but also a timing issue because of the many delays caused by the defendants actions and the extraordinary time it takes to fly to Amsterdam and the logistics of setting up the necessary working space there. The Court has resisted multiple requests from the PSC on this issue, primarily on the basis that the Court had an inadequate basis for requiring it. Based on the Court's findings above, the bad faith of the defendants in withholding discovery until well after it was required to be produced, by many months, the prejudice those delays have caused the litigation herein in postponing depositions and precipitating countless hours of chambers time and courtroom time discussing and advocating issues that did not need to occur, the Court finds an appropriate sanction pursuant to its inherent powers to be to require the defendants to produce all employees for deposition in the United States. Effective immediately or as close as logistically possible thereto, understanding that depositions and teams may already be in place, depositions shall take place in New York City or such other place as the PSC, and the defendants shall unanimously agree upon. If no alternative is unanimously agreed upon, they the Court's selection shall stand.

The PSC also requested a corporate fine as well as individual fines to be paid by each defense counsel. The corporate fine sought by plaintiffs is in the nature of $20 million. In the course of their advocacy, plaintiffs argued, in essence, that the Court's last sanction, was laughable and urged the Court to put some teeth in its sanction this time. The Court did note a sigh of relief on the faces of the corporate general counsel, though no laughs from the defense side of the courtroom. The Court is not moved by such advocacy. Moreover, the Court is not generally inclined to impose sanctions. In this judge's recollection, perhaps three times in seven years on the state bench and perhaps twice in fifteen years as a federal

judge, this order being the third. No judge should relish the serious obligation associated with a sanction, however, when a Court is confronted with a situation such as the instant one, it must act. But when it acts, it must do so in measured terms and in proportion to the wrongs and the prejudice before it. The wrongs here are egregious in the eyes of the Court. As hereinbefore provided, there may be more orders yet to come; orders which take actions designed to determine what aspects of the plaintiffs' case have been prejudiced or even so damaged as to interfere with their ability to prove what they legally have to prove and for the facts of this case to come out. Going forward, based on the findings heretofore, pursuant to the Court's inherent powers, and to encourage defendants to respect this Court and comply with its orders, the Court fines both defendants, jointly and severally, $931,500.00 ($500.00 per case). The last time the Court imposed a sanction it was based on a figure around $25,000.00. The Court assessed a figure at $20.00 per case for the number of cases then pending (the total ended up being $29,500.00). Then as now, the Court's imposition of a fine is a measured action, designed to let the defendants know that the Court's order and the Court deserve respect. If a somewhat forceful reminder of those tenants in the law must be sent to defendants for their misdeeds which demonstrate something to the contrary, so be it. Never should such reminders shock any one's conscience. Here, the first one was quite modest indeed. It did not send a sufficient message, but then most if not all the deeds the Court discussed herein were well underway, just not discovered. The fine imposed today, will not impact the defendants profit margins, but hopefully together with the potential future actions the Court may be forced to take, once it learns whether the plaintiffs have been so prejudiced by this misconduct as to be unable to fully prosecute their cases, the defendants will understand once and for all time compliance with the Court's orders is not an optional part of litigation strategy. Just as the Court did not exhaust what it has available to it in this instance, as the plaintiffs urged in the first sanction hearing, its measured approach to behavior modification leaves remedies yet to be addressed should defendants continue on the path of wrongheaded litigation strategy as the Court has sanctioned herein.

***21 SO ORDERED:**

S.D.Ill., 2013
In re Pradaxa (Dabigatran Etexilate) Products Liability Litigation
Not Reported in F.Supp.2d, 2013 WL 6486921 (S.D.Ill.)

END OF DOCUMENT

Slip Copy, 2014 WL 4100615 (S.D.N.Y.)
(Cite as: 2014 WL 4100615 (S.D.N.Y.))

United States District Court,
S.D. New York.
BROADSPRING, INC., Plaintiff,
v.
CONGOO, LLC, d/b/a Adiant, et al., Defendants.

No. 13–CV–1866 (JMF).
Signed Aug. 20, 2014.

OPINION AND ORDER

JESSE M. FURMAN, District Judge.

***1** This is a lawsuit between bitter rivals in the online advertising industry. Plaintiff Broadspring, Inc. ("Broadspring") brought the action against its competitor, Congoo, LLC ("Congoo"), and two Congoo executives, Chief Executive Officer, Ashraf Nashed, and Senior Vice President of Business Development, Rafael Cosentino (collectively, "Defendants"). Broadspring alleges principally that Defendants engaged in a campaign to spread false and defamatory information about it through Internet posts and other communications. Congoo, in turn, has brought counterclaims alleging that Broadspring made false and misleading statements about Congoo to two of its clients. (Am. Compl. (Docket No. 27); Answer & Am. Countercls. (Docket No. 45)). Before the Court are seven different motions, including cross-motions for summary judgment, dueling motions to exclude the testimony of expert witnesses at trial, two motions by Plaintiff for discovery-related sanctions, and a motion by Plaintiff for leave to file a Second Amended Complaint. (Docket Nos. 75, 94, 97, 98, 102, 108).

For the reasons stated below, Defendants' motion for summary judgment is denied except with respect to the tortious interference claim against Defendant Nashed. In addition, Plaintiff's motion for summary judgment is granted. Further, Plaintiff's motion to exclude is granted in part and denied in part, and Defendants' motion to exclude is denied. Finally, Plaintiff's motion for sanctions based on improper designations of material as highly confidential is granted, Plaintiff's motion for sanctions based on spoliation of evidence is granted in part and denied in part, and Plaintiff's motion seeking leave to file a Second Amended Complaint is granted. The end result is that, but for the tortious interference claim against Defendant Nashed, all of Plaintiff's affirmative claims remain, and all of Congoo's counterclaims are dismissed.

BACKGROUND

A. The Parties

As noted, Broadspring and Congoo are competitors in the online advertising business. (Markiles Decl. (Docket No. 141) ¶ 3; Nashed Decl. (Docket No. 104) ¶ 10). They each operate online advertising networks, which connect advertisers with websites, or "publishers." (Markiles Decl. ¶ 3). Online advertising networks place their advertisers' advertisements on publishers' websites, generating revenue from the advertisers and, in turn, paying publishers for the space. (*Id.*). The online advertising networks pay publishers either on a "CPM" basis—that is, a fixed sum per every thousand impressions (or viewers) that an advertisement receives—or on a "revenue share" basis, whereby the publisher receives a percentage of the revenue the advertising network derives from its advertisers. (*Id.*).

Broadspring is a Delaware corporation whose sole office is in Irvine, California. (*Id.* ¶ 1). It was incorporated in 2002, but had no revenue prior to June 2004, at which point it acquired the assets of another company, Mindset Interactive, Inc. (Alexander Decl. Supp. Defs.' Mot. Summ. J. (Docket No. 111), Ex. 4

("Markiles Dep.") 38:16–40:2; Alexander Decl. Supp. Defs.' Mot. Summ. J., Ex. 8 ("Jatwani Dep.") 27:5–11; Alexander Decl. Supp. Defs.' Mot. Summ. J., Ex. 21). Congoo, which launched its online advertising business in 2008 and also operates under the names Adiant and Adblade, is a Delaware limited liability company whose principal place of business is in Somerville, New Jersey. (Nashed Decl. ¶¶ 2–3). As noted, Nashed is Congoo's Chief Executive Officer and Cosentino is its Senior Vice President of Business Development. (*Id.* ¶¶ 1, 9).

B. The Squidoo Lens and Its Dissemination

***2** The dispute between the parties centers on a web page that Defendant Cosentino created in mid-February 2013 on the website www.squidoo.com, which is a platform that allows users to create pages, or "lenses," on subjects of their choice. (Cosentino Decl. (Docket No. 105) ¶ 2; Godin Decl. (Docket No. 106) ¶ 2). Under the moniker "Recruiterman"—whose profile page states that the account holder "live[s] in Brooklyn with [his] wife Susan and [their] 4 year [ ] old boy Liam," none of which applies to Cosentino—Cosentino created a page (the "Lens") on the topic of online advertising and marketing businesses. (Cosentino Decl. ¶ 2; Katz Decl. Opp'n Defs.' Mot. Summ. J. (Docket No. 143), Ex. 3; Alexander Decl. Supp. Defs.' Mot. Summ. J., Ex. 3 ("Cosentino Dep.") 252:24–253:22).[FN1] The Lens provided Cosentino's commentary—without disclosing his identity or his relationship to Congoo—on thirteen different advertising networks, including Broadspring and Congoo. (Katz Decl. Opp'n Defs.' Mot. Summ. J., Ex. 4). In its first iteration, the Lens stated that "many of [Broadspring's] advertisers appear to be continuity programs (re-bill offers) where the advertiser gets the customer to enter their credit card for a free trial and the[n] makes it tough to cancel. I'd be careful here." (*Id.* at 3).

FN1. Plaintiff represents that the Recruiterman profile page indicates that the account holder's name is Jonathan Tovar, but the screenshot of the page submitted to the Court does not show the account holder's name. (*See* Katz Decl. Opp'n Defs.' Mot. Summ. J., Ex. 3). In his deposition, Cosentino did not appear to contest that the Lens was posted under the name Jonathan Tovar, and admitted that he knows no one with that name. (Cosentino Dep. 198:14–199:16, 254:3–16).

On February 23, 2013, Cosentino e-mailed Nashed a link to the Lens, to which Nashed replied: "Ingenious!" (Katz Decl. Opp'n Defs.' Mot. Summ. J., Ex. 5). On March 2, 2013, Nashed sent Cosentino another e-mail, which contained additional statements about Broadspring. (Cosentino Decl. ¶ 13). Among other things, Nashed wrote that "it looks like Broadspring was formerly Mindset Interactive, a notorious spyware company. Mindset was eventually shut down by the [Federal Trade Commission ("FTC")] and Sanford Wallace, their founder, known as 'Spamford Wallace' was banned from online activity for 5 years." (Katz Decl. Opp'n Defs.' Mot. Summ. J., Ex. 6). Toward the end of the e-mail, Nashed wrote "[o]ur publishers should know about [Broadspring's] background." (*Id.*). Cosentino reviewed the e-mail, performed some "Google searches of [his] own," and then revised the Lens that same day. (Cosentino Decl., ¶ 14–15). The updated version of the Lens contained text that was nearly identical to the text of Nashed's e-mail. Under the "Broadspring" header, the revised Lens read:

> A simple Google search shows that Broadspring was formerly Mindset Interactive, a notorious spyware company. Mindset was eventually shut down by the FTC in 2005 and Sanford Wallace, their founder, known as "Spamford Wallace" was banned from online activity for 5 years. In Nov 2006, Broadspring's shareholders then launched the notorious ringtones company, New Motion, dba Atrinsic. Atrinsic had $17mm in financing (from various unknown investors), became public through a shady reverse-merger. They settled 3 years ago with 6 million users scammed: http://

www.ftc.gov/os/caselist/0423142/WallaceFinalJudgment.pdf

***3** (Katz Decl. Opp'n Defs.' Mot. Summ. J., Ex. 7). On March 4, 2013, Cosentino sent Nashed a link to the Lens using his Yahoo! Instant Messenger account. (*Id.*, Ex. 8; Cosentino Decl. ¶ 24).

Cosentino disseminated the Lens, as well as statements similar to those made in the Lens, in several ways. First, he posted links to the Lens in discussion threads on other websites under false names. (*See, e.g.*, Katz Decl. Opp'n Defs.' Mot. Summ. J., Ex. 9, at 2; *Id.*, Ex. 10, at 5; Cosentino Dep. 289:6–20, 293:6–294–22). Second, he e-mailed links to the Lens directly to publishers, including Intermarkets.net, the New Hampshire Union Leader, the New York Daily News, and Geology.com. (Katz Decl. Opp'n Defs.' Mot. Summ. J., Ex. 11, at 8; *Id.*, Ex. 12, at 5; *Id.*, Ex. 13, at 2; *Id.*, Ex. 14, at 2; Cosentino Decl. ¶ 26). Third, although Squidoo "locked" the Lens on March 11, 2013 (making it inaccessible to the public) (Godin Decl. ¶ 7; Katz Decl. Opp'n Defs.' Mot. Summ. J., Ex. 15), Cosentino pseudonymously re-posted many of the statements that were on the Lens in a discussion thread on another website, Contextly.com. Under the name "Richard J," for example, Cosentino posted the following:

> [Broadspring] used to distribute spyware under the company name Mindset Interactive. When they were named in a lawsuit by the FTC they dropped that name. They then formed a new company called Atrinsic dba New Motion which distributed Ring tone scams to 13 year olds. They were again sued and this time had to settle a class action lawsuit with 6 Million people. Now Broadspring is using content.ad to drive consumer[ ] to howlifeworks and those fake editorials which are not even marked as such so they can get their credit cards and re-bill them. Publishers who work with these guys simply have zero critical thinking or care[ ] about their audience.

(Katz Decl. Opp'n Defs.' Mot. Summ. J., Ex. 16, at 10–11; Cosentino Dep. 300:12–19). Even after posting on Contextly.com, Cosentino continued to e-mail similar statements to publishers directly. (*See, e.g.*, Katz Decl. Opp'n Defs.' Mot. Summ. J., Ex. 18, at 149 ("So you know, the folks at Broadspring shut down their company (mindset interactive) soon after they were named by the FTC in a lawsuit for distributing spyware.")).

C. Geology.com

One publisher that is particularly relevant to the parties' claims is Geology.com. In June 2012, Congoo and Geology.com had entered into an agreement that provided Congoo with the exclusive right to serve advertisements "with a thumbnail image and/or a title and/or a description and/or a call to action" on Geology.com. (Alexander Decl. Supp. Defs.' Mot. Summ. J., Ex. 40). The agreement provided that it could be terminated with ninety days of notice. (*Id.*). In February 2013, without either party terminating the agreement, Geology.com began to run Broadspring advertisements as well as the Congoo advertisements. (Pl.'s Response to Defs.' Rule 56.1 Statement (Docket No. 144) ("Pl.'s Rule 56.1 Statement Response") ¶ 75; Alexander Decl. Supp. Defs.' Mot. Summ. J., Ex. 41, at 5). Apparently, Cosentino saw the Broadspring advertisements; he then called Hobart King, the principal of Geology.com, on March 5, 2013, and stated that King "could get in trouble running those ads." (Katz Decl. Opp'n Defs.' Mot. Summ. J., Ex. 19 ("King Dep.") 74:9–17). Cosentino also told King that Broadspring had "gotten in trouble for spyware" and that it had been "in court over something." (*Id.* at 74:1975:3). Later that day, Cosentino e-mailed King a link to the Lens, which he told King he could read to "get a review on Broadspring ads and other ad networks." (*Id.* at 77:23–78:2; Katz Decl. Opp'n Defs.' Mot. Summ. J., Ex. 14, at 2).[FN2]

FN2. Cosentino did not tell King who wrote the Lens. In fact, King appears to have been

> unaware that Cosentino authored the Lens until he was informed of that fact at his deposition. (King Dep., 80:3–11).

***4** Within the next few days, Geology.com terminated its dealings with Broadspring. In fact, the very day that that Cosentino called King and sent him the Lens, King's webmaster was in the midst of replacing Congoo's advertisements with Broadspring advertisements. (King Dep. 80:18–23). After King received Cosentino's e-mail, however, he "changed his mind," and told his webmaster to put the Congoo advertisements back up. (*Id.* at 81:4–11; Pl.'s Rule 56.1 Statement Response ¶ 77). Although the precise reasons for King's decision are in dispute, King testified that he changed his mind "mainly" because he was "concerned about what he had read [in the Lens], and [because he] was concerned about spyware." (King Dep. 81:13–15; *see also* Alexander Decl. Supp. Defs.' Mot. Summ. J., Ex. 41, at 14 (King responding to an e-mail from Brett Houck, a business development manager at Broadspring, who asked what Broadspring could do to get its advertisements put back up on Geology.com, by saying "[s]omeone sen[t] me a link to [the Lens]," and that he was therefore "hesitant to run the ads after seeing the above").

D. Procedural History

Plaintiff filed its initial Complaint on March 20, 2013 (Docket No. 1), and then filed the Amended Complaint on April 24, 2013 (Docket No. 27). The Amended Complaint asserts a Lanham Act claim, a defamation claim, and a tortious interference claim. (*Id.*, at 7–8). Defendants filed their Answer on April 11, 2013, which asserted Lanham Act, defamation, and tortious interference counterclaims, all based on allegations that Broadspring "systematically solicited publishers, including Readers Digest, Geology.com, Tech Media, World Now, and The Journal Register Company (the 'Congoo Clients'), from whom Congoo purchases space." (Answer & Countercls. (Docket No. 26) ¶¶ 48, 56, 63). On July 26, 2013, Defendants amended their Answer and Counterclaims, limiting the "Congoo Clients" to Reader's Digest and Geology.com, and only asserting causes of action for tortious interference and unfair competition. (Am. Answer & Countercls. (Docket No. 45) ¶¶ 45–56).

As noted, there are seven motions presently before the Court. They include: (1) Defendants' motion for summary judgment, which seeks dismissal of the claims against them and judgment in their favor on the unfair competition counterclaim (Docket No. 97); (2) Plaintiff's motion for summary judgment or, alternatively, judgment on the pleadings, seeking to dismiss Defendants' counterclaims (Docket No. 108); (3) Plaintiff's motion to preclude Defendants' expert, Lance James, from testifying at trial (Docket No. 102); (4) Defendants' motion to preclude Plaintiff's expert, Marty Lafferty, from testifying at trial (Docket No. 94); (5) Plaintiff's motion, filed *in camera*, for sanctions based on the improper designation of documents as "Highly Confidential—Attorneys' Eyes Only" ("AEO"); (6) Plaintiff's motion for sanctions based on the spoliation of evidence, namely the failure to preserve instant messages (Docket No. 98); and (7) Plaintiff's motion seeking leave to file a Second Amended Complaint (Docket No. 75). For the reasons that follow, Defendants' motion for summary judgment is denied, except with respect to the tortious interference claim against Defendant Nashed, and Plaintiff's motion for summary judgment is granted. Further, Plaintiff's motion to exclude is granted in part and denied in part and Defendants' motion to exclude is denied. Finally, Plaintiff's motion for sanctions based on improper designations is granted, Plaintiff's motion for sanctions based on spoliation of evidence is granted in part and denied in part, and Plaintiff's motion seeking leave to file a Second Amended Complaint is granted.

SUMMARY JUDGMENT MOTIONS

***5** The Court first addresses the motions for summary judgment. Summary judgment is appropriate where the admissible evidence and the pleadings demonstrate "no genuine dispute as to any material

fact and the movant is entitled to judgment as a matter of law." Fed.R.Civ.P. 56(a). A dispute over an issue of material fact qualifies as genuine if the "evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Anderson v.. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). In ruling on a motion for summary judgment, all evidence must be viewed "in the light most favorable to the non-moving party," *Overton v. N.Y. State Div. of Military & Naval Affairs*, 373 F.3d 83, 89 (2d Cir.2004), and a court must "resolve all ambiguities and draw all permissible factual inferences in favor of the party against whom summary judgment is sought," *Sec. Ins. Co. of Hartford v. Old Dominion Freight Line, Inc.*, 391 F.3d 77, 83 (2d Cir.2004). When, as here, both sides move for summary judgment, a court is "required to assess each motion on its own merits and to view the evidence in the light most favorable to the party opposing the motion, drawing all reasonable inferences in favor of that party." *Wachovia Bank, Nat'l Ass'n v. VCG Special Opportunities Master Fund, Ltd.*, 661 F.3d 164, 171 (2d Cir.2011). Thus, "neither side is barred from asserting that there are issues of fact, sufficient to prevent the entry of judgment, as a matter of law, against it." *Heublein, Inc. v. United States*, 996 F.2d 1455, 1461 (2d Cir.1993).

"In moving for summary judgment against a party who will bear the ultimate burden of proof at trial, the movant's burden will be satisfied if he can point to an absence of evidence to support an essential element of the nonmoving party's claim." *Goenaga v. March of Dimes Birth Defects Found.*, 51 F.3d 14, 18 (2d Cir.1995); *accord PepsiCo, Inc. v. Coca–Cola Co.*, 315 F.3d 101, 105 (2d Cir.2002). By contrast, to defeat a motion for summary judgment, the nonmoving party must advance more than a "scintilla of evidence," *Anderson*, 477 U.S. at 252, and demonstrate more than "some metaphysical doubt as to the material facts," *Matsushita Elec. Indus. Co., Ltd. v. Zenith Radio Corp.*, 475 U.S. 574, 586 (1986). The non-moving party "cannot defeat the motion by relying on the allegations in [its] pleading or on conclusory statements, or on mere assertions that affidavits supporting the motion are not credible." *Gottlieb v. Cnty. of Orange*, 84 F.3d 511, 518 (2d Cir.1996) (citation omitted). Affidavits submitted in support or in opposition to summary judgment must be based on personal knowledge, must "set forth such facts as would be admissible in evidence," and must show "that the affiant is competent to testify to the matters stated therein." *Patterson v.. Cnty. of Oneida*, 375 F.3d 206, 219 (2d Cir.2004).

A. Plaintiff's Claims

The Court begins with Defendants' summary judgment motion to the extent that it seeks dismissal of Plaintiff's claims. Defendants move to dismiss Plaintiff's defamation claim, its Lanham Act claim, and its tortious interference claim. The Court addresses each in turn.

1. Plaintiff's Defamation Claim

a. Choice of Law

***6** The Court begins with Plaintiff's defamation claim. Before considering Defendants' arguments, the Court must first determine the source of law that applies. As this Court sits in New York, it must apply the New York choice-of-law analysis, *see Klaxon Co. v. Stenton Elec. Mfg. Co.*, 313 U.S. 487, 496 (1941), which first asks whether there is an "actual conflict of laws," *Condit v. Dunne*, 317 F.Supp.2d 344, 352 (S.D.N.Y.2004). The two potential sources of defamation law—California and New York (*compare* Pl.'s Mem. Opp'n Defs.' Mot. Summ. J. (Docket No. 140) 8–10 *with* Defs.' Reply Mem. Supp. Defs.' Mot. Summ. J. (Docket No. 158) 2–4)—do indeed conflict, as New York law grants opinions greater protection from defamation actions than California law does. *Condit*, 317 F.Supp.2d at 352. Accordingly, the Court must decide which state's law applies.

In tort actions such as this one, New York applies

the law of the state with the "most significant interest in the litigation." *Lee v. Bankers Trust Co.*, 166 F.3d 540, 545 (2d Cir.1999). In weighing those interests, New York courts distinguish between conflicts regarding "conduct-regulating" rules and conflicts regarding "loss-allocating" rules. *Id.* Defamation law regulates conduct, so the rule is to apply "the law of the place of the tort (*'lex loci delicti'*)." *Id.; see also Condit*, 317 F.Supp.2d at 353. In this case, however, it is not obvious where the tort occurred, as the Lens was posted on the Internet and was thus accessible nationwide. As one court has observed, "in cases where a defamatory statement is published nationally," as here, "it is not immediately apparent how one might identify 'the place' where the tort of defamation occurred." *Adelson v. Harris*, 973 F.Supp.2d 467, 477 (S.D.N.Y.2013); *see also Condit*, 317 F.Supp.2d at 353 ("In a defamation case where the statements at issue are published nationwide ... the locus of the tort factor begs, rather than answers, the ultimate choice of law question."). In such cases, there is a presumptive rule that the law of the plaintiff's domicile applies. *See, e. g., Adelson*, 973 F.Supp.2d at 477; *see also Reeves v. Am. Broad. Co., Inc.*, 719 F.2d 602, 605 (2d Cir.1983) (noting that "the state of the plaintiff's domicile will usually have the most significant relationship to the case"); *Davis v. Costa–Gavras*, 580 F.Supp. 1082, 1091 (S.D.N.Y.1984) ("In a libel case, the state of most significant relationship is usually the state where the plaintiff was domiciled at the time, if the libel was published in that state, since that is where he is presumed to have been most injured."). Here, that would mean the law of California—where Broadspring is domiciled. (Markiles Decl. ¶ 1). *See also, e.g., Dargahi v. Hymas*, No. 05–CV–8500 (BSJ), 2008 WL 8586675, at *5 (S.D.N.Y. Oct. 15, 2008) ("Under New York law, the domicile of a corporation for choice-of-law purposes is the State where it maintains its principal place of business." (internal quotation marks omitted)).

***7** To be sure, the presumptive rule in favor of the law of the plaintiff's domicile "does not hold true if ... some other state has a more significant relationship to the issue or the parties." *Adelson*, 973 F.Supp.2d at 477 (internal quotation marks omitted). But in this case, there is no basis to conclude that New York (or any other state) has a more significant relationship to the defamation claims than California. (*See* Defs.' Reply Mem. Supp. Defs.' Mot. Summ. J. 2–4). California has an obvious interest in protecting its citizens from defamatory statements. *See Adelson*, 973 F.Supp.2d at 478 (noting that Nevada, the state where plaintiff's business was based, "has an interest in protecting its citizens from tortious conduct"); *Condit*, 317 F.Supp.2d at 353 ("[T]he state of the plaintiff's domicile has an interest in protecting its citizens from defamation."). New York, on the other hand, has an interest in protecting the First Amendment rights of its citizens, *see, e. g., Adelson*, 973 F.Supp.2d at 478, but no Defendant is a citizen or resident of New York. (Nashed Decl. ¶ 2 (indicating that Congoo is incorporated in Delaware and its principal place of business is in New Jersey); Cosentino Dep. 253:11–13 (indicating that Cosentino resides in New Jersey); Am. Compl. ¶ 4 (alleging that Nashed is a citizen of New Jersey)). Neither the fact that Plaintiff filed suit in New York nor the fact that Defendant Cosentino did "much of the drafting ... of the Squidoo Lens ... while [he] was in New York" (Cosentino Reply Decl. (Docket No. 160) ¶ 2) is sufficient, by itself, to displace the presumption that California law should apply. *See Adelson*, 973 F.Supp.2d at 472, 477–79 (applying the law of Plaintiff's domicile, Nevada, over the law of the District of Columbia, even though the allegedly defamatory statements were published by an organization whose principal place of business was in the District of Columbia); *cf. Hatfill v. Foster*, 401 F.Supp.2d 320, 324–25 (S.D.N.Y.2005) (after surveying libel cases between out-of-state plaintiffs and New York defendants, finding a "marginal preference" for the law of the plaintiff's domicile, and noting that "where defendant's domicile trumped plaintiff's, New York had some other significant connection to the case"), *rev'd on reconsideration*, 415 F.Supp.2d 353 (S .D.N.Y.2006). Accordingly, the

Court will evaluate the defamation claim under California law. [FN3]

> FN3. Although California law applies to the defamation claim, the parties do not dispute that the law of the Second Circuit applies to the Lanham Act claim or that New York law applies to the tortious interference claim. *See In re Horizon Cruises Litig.*, 101 F.Supp.2d 204, 207 n. 1 (S.D.N.Y.2000) ([C]hoice of law determinations are made on a claim-by-claim basis."). The Court will thus analyze those claims accordingly.

b. Plaintiff's Claim Under California Law

Defendants advance two main arguments as to why Broadspring's defamation claim should be dismissed. First, Defendants argue that they are immune from liability because the Lens is a constitutionally protected opinion under the First Amendment. (Defs .' Mem. Supp. Defs.' Mot. Summ. J. (Docket No. 100) 5–10; Defs.' Reply Mem. Supp. Defs.' Mot. Summ. J. 4–7). Second, they contend that they have successfully raised the "substantial truth" defense. (Defs.' Mem. Supp. Defs.' Mot. Summ. J. 10–17; Defs.' Reply Mem. Supp. Defs.' Mot. Summ. J. 8–11). The Court finds both arguments for summary judgment without merit.

***8** As a general rule, "[a]lthough statements of fact may be actionable as libel, statements of opinion are constitutionally protected." *McGarry v. Univ. of San Diego*, 64 Cal.Rptr.3d 467, 479 (Cal.Ct.App.2007) (citing *Baker v. Los Angeles Herald Examiner*, 721 P.2d 87, 90 (Cal.1986)). Statements that are simply "couch[ed] ... in terms of opinion," however, are not protected, as they may still "imply a false assertion of fact." *Milkovich v. Lorain Journal Co.*, 497 U.S. 1, 18–19 (1990). To distinguish between constitutionally protected expressions of opinion and actionable assertions of fact, California courts ask "whether a reasonable fact finder could conclude the published statement declares or implies a provably false assertion of fact." *McGarry*, 64 Cal.Rptr.3d at 479; *see also Summit Bank v. Rogers*, 142 Cal.Rptr.3d 40, 59–60 (Cal.Ct.App.2012) (similar); *Nygard, Inc. v. Uusi–Kerttula*, 72 Cal.Rptr.3d 210, 226 (Cal.Ct.App.2008) (similar). In conducting that inquiry, courts consider the "totality of the circumstances," including the language of the statement and the context in which the statement was made. *Franklin v. Dynamic Details, Inc.*, 10 Cal.Rptr.3d 429, 436–37 (Cal.Ct.App.2004).

Here, there is no question that Defendants' statements about Broadspring imply provably false factual assertions. For example, the Lens affirmatively asserts that "Broadspring was formerly Mindset Interactive," which was "shut down by the FTC in 2005." (Katz Decl., Ex. 7). Whether Broadspring or Mindset Interactive was "shut down by the FTC in 2005" is plainly a provably false assertion of fact, and a preface that the assertion was revealed by "[a] simple Google search" does not render it constitutionally protected opinion. *See Weller v. Am. Broad. Cos.*, 283 Cal.Rptr. 644, 652 (Cal.Ct.App.1991) ("[W]e reject the notion that merely couching an assertion of a defamatory fact in cautionary language such as 'apparently' or 'some sources say' ... necessarily defuses the impression that the speaker is communicating an actual fact."). To cite another example, the Lens states that "Sanford Wallace, their founder, known as 'Spamford Wallace' was banned from online activity for 5 years." (Katz Decl., Ex. 7). Among other things, that statement clearly implies the provably false assertion that Sanford Wallace was the founder of either Broadspring or Mindset Interactive. In addition, Cosentino repeated the assertion regarding Broadspring being sued or shut down by the FTC in the Contextly.com posting (Katz Decl. Opp'n Defs.' Mot. Summ. J., Ex. 16, at 10–11; Cosentino Dep. 300:12–19), and in an e-mail to publisher KSL/Deseret News (Katz Decl., Ex. 32).

Further, Defendants' contention that the Lens, "taken as a whole," is a non-actionable opinion is baseless. (Defs.' Mem. Supp. Defs.' Mot. Summ. J.

5–8). Putting aside the fact that the Lens is just one of numerous places where Defendants made assertions about Broadspring, the Lens is not at all akin to the rankings that the Eastern District of Tennessee deemed non-actionable in *Seaton v. TripAdvisor, LLC*, No. 11–CV–549, 2012 WL 3637394, at *7 (E.D.Tenn. Aug. 22, 2012), *aff'd*, 728 F.3d 592 (6th Cir.2013). In *Seaton*, the allegedly defamatory statement was TripAdvisor.com's "2011 Dirtiest Hotels" list, a rank ordering of the purportedly ten dirtiest hotels in the United States according to the site's users. *Id.* at *2. Although the Lens does provide rankings for each of the thirteen advertising networks it discusses (*see* Katz Decl., Ex. 7), it contains specific, detailed, and provably false factual assertions about the networks as well, including, as relevant here, Broadspring.

***9** Defendants' second argument—namely, that the statements in the Lens are substantially true—fares no better. In general, "[t]he burden of pleading and proving truth is on the defendant." *Smith v. Maldonado*, 85 Cal.Rptr.2d 397, 403 n. 5 (Cal.Ct.App.1999). Congoo argues that the burden has shifted here because Broadspring is a "limited purpose public entity." (Defs.' Reply Mem. Supp. Defs.' Mot. Summ. J. 8 n. 10). But that argument is without merit. The essence of the limited public purpose doctrine is that if there is a "public controversy," and the plaintiff has "undertaken some voluntary act through which he or she sought to influence resolution of the public issue," the burden shifts to the plaintiff to prove that the allegedly defamatory statement was made with knowledge of falsity or reckless disregard for truth. *Ampex Corp. v. Cargle*, 27 Cal.Rptr.3d 863, 869–70 (Cal.Ct.App.2005). But here, the public controversy into which Broadspring is alleged to have inserted itself is the very controversy that Congoo created—namely, the truth of the allegations made in the Lens. (*See* Defs.' Reply Mem. Supp. Defs.' Mot. Summ. J. 8 n. 10 (citing Alexander Reply Decl., Ex. 4)). A defendant cannot "create a public controversy simply by publishing an article that put plaintiff's behavior in the spotlight." *Carver v. Bonds*, 37 Cal.Rptr.3d 480, 501 (Cal.Ct.App.2005); *see also Hutchinson v. Proxmire*, 443 U.S. 111, 135 (1979) ("[T]hose charged with defamation cannot, by their own conduct, create their own defense by making the claimant a public figure."). Accordingly, there is no "public controversy" for purposes of the limited public purpose doctrine, and it is Defendants' burden to establish the truth of their statements.

Defendants have come nowhere close to doing so. To the contrary, the evidence submitted indicates that many of the statements were indeed false. For example, neither Broadspring nor Mindset was ever sued or "shut down" by the FTC. (Markiles Decl. ¶ 12). Instead, the FTC investigated Sanford Wallace for his marketing and software distribution practices, and Wallace was a third-party software distributor of Mindset's. (Jatwani Dep. 70:1118, 84:23–85:11). Ultimately, the investigation resulted in a default judgment being entered against Wallace and his corporation SmartBot.Net (Alexander Decl. Supp. Defs.' Mot. Summ. J., Ex. 18), but neither Broadspring nor Mindset was named as a defendant in the case. Further, Broadspring's decision to exit the business of software distribution was entirely voluntary, and motivated by concerns that the behavior of third-party distributors such as Wallace would be "difficult to police ... adequately." (Markiles Dep. 83:2–11). Even further from the truth is the Lens's assertion that Wallace was "their founder"—"their" referring to Broadspring, Mindset, or both. (Katz Decl., Ex. 7). Defendants do not even attempt to argue that that statement is true, but meekly suggest that Wallace and Broadspring were "connected" as "business partners." (Defs.' Mem. Supp. Defs.' Mot. Summ. J. 14). The difference between being the founder of a company and being "connected" as a business partner of a company, however, is far greater than the "slight inaccuracy in the details" that is permitted for the substantial truth defense under California law. *See Gilbert v. Sykes*, 53 Cal.Rptr.3d 752, 765 (Cal.Ct.App.2007) (noting that inaccuracies are permitted only if they "do[ ] not change the complexion of the affair so as to

affect the reader of the [publication] differently" (internal quotation marks omitted)).

***10** Finally, the Court rejects Defendants' contention that the defamation claim fails against Nashed and Congoo because they "did not author or publish the Lens." (Defs.' Mem. Supp. Defs.' Mot. Summ. J. 7 n. 2). To support a claim for defamation against Nashed, Plaintiff needs to establish only that Nashed "took a 'responsible part' in the publication of the defamatory matter," which includes "participating in the publication of an article." *Hawran v. Hixson*, 147 Cal.Rptr.3d 88, 105 (Cal.Ct.App.2012). Here, a reasonable jury could conclude that Nashed took a "responsible part" in the Lens's publication based on the e-mail exchange between Cosentino and Nashed, the updated version of the Lens posted on March 2, 2013, and Cosentino's admission that he "updated [the] Lens ... with some of the information" in the e-mail from Nashed. (Katz Decl., Ex. 5; *Id.*, Ex. 6; *Id.*, Ex. 7; Cosentino Dep. 219:11–220:4). In addition, given the nature of the statements, Cosentino's and Nashed's senior roles at Congoo, and the fact that the two communicated about the Lens using their company e-mail addresses, a reasonable jury could hold Congoo liable for the allegedly defamatory statements on a *respondeat superior* theory. *See Rivera v. Nat'l R.R. Passenger Corp.*, 331 F.3d 1074, 1080 (9th Cir.2003) (noting, that under California law, an employer may be held liable for an employee's defamatory statement "[a]s long as the statement was made within the scope of employment"); *see also Kelly v. Gen. Tel. Co.*, 186 Cal.Rptr. 184, 186 (Cal.Ct.App.1982) (similar).

2. Plaintiff's Lanham Act Claim

The Court next turns to Plaintiff's Lanham Act claim. Section 43(a) of the Lanham Act provides that

> [a]ny person who ... in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities, shall be liable in a civil action by any person who believes that he or she is likely to be damaged by such act.

15 U.S.C. § 1125(a)(1)(B). For a representation to qualify as "commercial advertising or promotion," it must be: "(1) commercial speech, (2) made for the purpose of influencing consumers to buy defendant's goods or services, and (3) although representations less formal than those made as part of a classic advertising campaign may suffice, they must be disseminated sufficiently to the relevant purchasing public." *Gmurzynska v. Hutton*, 355 F.3d 206, 210 (2d Cir.2004) (internal quotation marks omitted) (citing *Fashion Boutique of Short Hills, Inc. v. Fendi USA, Inc.*, 314 F.3d 48, 56, 57–58 (2d Cir.2002)). Here, Defendants contend that Plaintiff has not established sufficient dissemination of the allegedly misleading representations. (Defs.' Mem. Supp. Defs.' Mot. Summ. J. 18–21). The Court is not persuaded.

"[T]he touchstone of whether a defendant's act may be considered 'commercial advertising or promotion' ... is that the contested representations are part of an organized campaign to penetrate the relevant market." *Fashion Boutique*, 314 F.3d at 57. Although "isolated disparaging statements" do not suffice, *id.; see also, e.g., Prof'l Sound Servs., Inc. v. Guzzi*, 349 F.Supp.2d 722, 729 (S.D.N.Y.2004) ("Dissemination of a statement to one customer out of 36 simply does not meet this standard."), the "breadth of dissemination, although important, is not dispositive," and "the primary focus is the degree to which the representations in question explicitly target relevant consumers," *Gordon & Breach Science Publishers S.A. v. Am. Inst. of Physics*, 905 F.Supp. 169, 182 (S.D.N.Y.1995). Here, Cosentino admits that he e-mailed links to the Lens itself to four publishers (Cosentino Decl. ¶ 26), and, after Squidoo locked the Lens, he continued to send those and other publishers both links to the Contextly.com article and e-mails with statements about Broadspring similar to those in the Lens (Katz Decl ., Ex. 18). Based on those communications, as well as Nashed's e-mailed statement to Cosentino that

"[o]ur publishers should know about [Broadspring's] background," a reasonable jury could conclude that Defendants' dissemination of the Lens, the Contextly.com article, and other e-mails were part of an organized campaign to penetrate the market of publishers. (*Id.*, Ex. 6).

***11** The Court also rejects Defendants' argument that the false advertising claim should be dismissed for failure to establish causation of damages. (Defs.' Mem. Supp. Defs.' Mot. Summ. J. 21–22). At a minimum, there is a genuine factual dispute as to why Geology .com terminated its relationship with Broadspring. According to Plaintiff, Geology.com removed Broadspring's advertising units because King reviewed the Lens after having been sent it Cosentino (Pl.'s Rule 56.1 Statement Response ¶ 77), an assertion that is supported by King's testimony (King Dep. 80:3–81:22), as well as an e-mail exchange between King and Alexander (Alexander Decl. Supp. Defs.' Mot. Summ. J., Ex. 41, at 14–18). By contrast, Defendants point to other factors that may have caused Geology.com to stop working with Plaintiff (*see* Defs.' Mem. Supp. Defs. Mot. Summ. J. 22), creating a factual dispute that is not appropriate for determination on summary judgment. Further, Plaintiff is not required to prove actual sales diversion in order to obtain the injunctive relief that it seeks. (Am.Compl.¶ 24). *See Johnson & Johnson v. Carter–Wallace, Inc.*, 631 F.2d 186, 191 (2d Cir.1980) ("Likelihood of competitive injury sufficient to warrant a § 43(a) injunction has been found in the absence of proof of actual sales diversion in numerous cases."). Accordingly, Plaintiff's Lanham Act claim survives.

3. Plaintiff's Tortious Interference Claim

Finally, the Court addresses Plaintiff's tortious interference claim. That claim is predicated on Defendants' alleged interference with Broadspring's relationship with Geology.com. (Am. Compl. ¶ 28; Pl.'s Mem. Opp'n Defs.' Mot. Summ. J. 33–34). Significantly, however, Plaintiff does not claim that Defendants caused the breach of an existing contractual relationship, but rather that they interfered with a prospective economic advantage. (Pl.'s Mem. Opp'n Defs.' Mot. Summ. J. 33–34 (citing Am. Compl. ¶ 28)). *See, e.g., Strapex Corp. v. Metaverpa N.V.*, 607 F.Supp. 1047, 1050 (S.D.N.Y.1985) ("Interference with a plaintiff's business relations with a third party can be found if the plaintiff had a reasonable expectancy of a contract with the third party, which can result from mere negotiations." (internal quotation marks omitted)). Accordingly, to establish its claim, Plaintiff must demonstrate that "(1) it had a business relationship with a third party; (2) the defendant knew of that relationship and intentionally interfered with it; (3) the defendant acted solely out of malice, or used dishonest, unfair, or improper means; and (4) the defendant's interference caused injury to the relationship." *State St. Bank & Trust Co. v. Inversiones Errazuriz Limitada*, 374 F.3d 158, 171 (2d Cir.2004) (internal quotation marks omitted).

As a threshold matter, the Court dismisses the tortious interference claim with respect to Defendant Nashed. (*See* Defs.' Mem. Supp. Defs.' Mot. Summ. J. 23 n. 10). The basis for the tortious interference claim is that Cosentino sent the Lens to King at Geology.com, prompting King to terminate Geology.com's dealings with Broadspring. (*See* King Dep. 74:9–78:2). There is no suggestion, let alone evidence, that Nashed had any contact with King, was aware of Cosentino's dealings with King, or otherwise interfered with Broadspring's relationship with Geology.com. (*See id.* 35:7–8 (Katz indicating that he is unfamiliar with Nashed)). Accordingly, the tortious interference claim against Nashed must be dismissed.

***12** With respect to Cosentino and Congoo, however, Defendants do not dispute that Plaintiff can satisfy the first two elements of a tortious interference claim. (*See* Defs.' Reply Mem. Supp. Defs.' Mot. Summ. J. 14–15). *See also Balance Point Divorce Funding, LLC v. Scrantom*, 978 F.Supp.2d 341, 350–51 (S.D.N.Y.2013) (holding that the plaintiff stated a claim for tortious interference with contract

under a vicarious liability theory). A reasonable jury could also find in Broadspring's favor on the third and fourth elements. It is well-established, for example, that conduct that amounts to an independent tort constitutes "wrongful means" for purposes of a tortious interference claim, *Carvel Corp. v. Noonan,* 3 N.Y.3d 182, 190 (2004), and the Court has already declined to dismiss Plaintiff's claim for defamation. Additionally, the Court has also concluded that a genuine dispute of material fact exists as to whether Defendants' statements to Geology.com caused the advertiser to terminate its relationship with Plaintiff. Defendants' reliance on the "economic interest" defense does not affect that analysis. (*See* Defs.' Mem. Supp. Defs.' Mot. Summ. J. 24–26; Defs.' Reply Mem. Supp. Defs.' Mot. Summ. J. 14–15). To be sure, "procuring the breach of a contract in the exercise of equal or superior right is ... justification for what would otherwise be an actionable wrong," *Foster v. Churchill,* 87 N.Y.2d 744, 750 (1996) (internal quotation marks and alterations omitted), and Congoo's exclusive contract with Geology.com (*see* Alexander Decl. Supp. Defs.' Mot. Summ. J., Ex. 40; Pl.'s Rule 56.1 Statement Response ¶ 73) did indeed give it the right to protect its economic interest, *see C.E.D. Mobilephone Commc'ns, Inc. v. Harris Corp.*, No. 81–CV–4651 (JFK), 1985 WL 193, at *7 (S.D.N.Y. Jan. 14, 1985) ("[Defendant's] exclusive ... agreement with [third party] ... gives [Defendant] the right to engage in otherwise wrongful interference with the ... contract."). The means with which Congoo was permitted to protect its economic interest, however, were limited to those not otherwise illegal, *see, e.g., Felsen v. Sol Cafe Mfg. Corp.*, 24 N.Y.2d 682, 686 (1969); *see also Murtha v. Yonkers Child Care Ass'n,* 45 N.Y.2d 913, 915 (1978) ("A corporate officer who is charged with inducing the breach of a contract between the corporation and a third party is immune from liability if it appears that he is acting in good faith as an officer and did not commit independent torts ..."), and here a reasonable jury could conclude that Defendants' authorship and dissemination of the Lens—the very acts that allegedly caused Geology.com to terminate its relationship with Broadspring—constituted defamation and Lanham Act false advertising. Accordingly, the economic interest defense may not be available to Defendants, and Plaintiff's tortious interference claim survives with respect to Consentino and Congoo.

B. Congoo's Counterclaims

***13** The Court turns now to Congoo's counterclaims, which allege that Broadspring made false and misleading statements to Reader's Digest and Geology.com in an effort to procure their business. (Answer & Am. Countercls. ¶ ¶ 45, 48). Specifically, Congoo alleges that Broadspring made two such statements. First, Congoo alleges that Broadspring misled the Publishers by telling them that its advertisements, or "creatives," were much "cleaner" than Congoo's, and failed to disclose—as required by FTC guidelines—that they are advertisements, and thus no "cleaner." (Defs.' Mem. Opp'n Pl.'s Mot. Summ. J. (Docket No. 136) 1; *see also* Defs.' Mem. Supp. Defs.' Mot. Summ. J. 27–30). Second, Congoo claims that Broadspring deceived the Publishers by telling them that Broadspring offered a higher CPM than Congoo when, in fact, "Broadspring [was] often unable to beat (or even meet) the CPMs paid by Congoo." (Answer & Am. Countercls. ¶ 48; Defs.' Mem. Opp'n Pl.'s Mot. Summ. J. 1). Congoo alleges that, as a result of making those statements, Reader's Digest and Geology.com sold Broadspring space on their websites, in breach of exclusive agreements that Congoo had with the two publishers. (Answer & Am. Countercls. ¶¶ 47, 50–51). On the basis of that conduct, Congoo brings counterclaims for both tortious interference and unfair competition. (*Id.* ¶¶ 45–56). Congoo now seeks judgment in its favor on the unfair competition counterclaim. (Defs.' Mem. Supp. Defs.' Mot. Summ. J. 27–30). Plaintiff cross-moves for summary judgment (or, alternatively, judgment on the pleadings) with respect to both counterclaims. (Docket No. 108).

Plaintiff has the better of the argument. Put simply, Congoo fails to adduce any evidence suggesting that Plaintiff's conduct was "improper," as

required for a tortious interference claim, *see White Plains Coat & Apron Co. v. Cintas Corp.*, 8 N.Y.3d 422, 426 (2007), or that Plaintiff acted in "bad faith," as required for an unfair competition claim, *see Jeffrey Milstein, Inc. v. Greger, Lawlor, Roth, Inc.*, 58 F.3d 27, 35 (2d Cir.1995). Congoo argues that those respective elements are met because Plaintiff's statements were "false" and "misleading" (Defs.' Mem. Opp'n Pl.'s Mot. Summ. J. 11, 19), but no rational jury could reach such a conclusion. Defendants characterize the "cleaner creatives" statement as misleading because it falsely suggested that Broadspring's advertisements complied with FTC disclosure guidelines (*Id.*, at 1; *see also* Defs.' Mem. Supp. Defs.' Mot. Summ. J. 27–30), but Congoo itself admits that the phrase "clean creatives" has a "broad definition" that could refer to a number of different features of the advertisement (Defs.' Mem. Opp'n Pl.'s Mot. Summ. J. 14–15). Notably, there is no evidence that representatives of Reader's Digest, Geology.com, or Broadspring understood the phrase as Defendants interpret it. (*See, e.g.*, Alexander Decl. Opp'n Pl.'s Mot. Summ. J. (Docket No. 137), Ex. 8 ("Sottile Dep.") 67:7–16 (stating that "cleaner creatives" means "less clutter" in the advertisement); Alexander Decl. Supp. Defs.' Mot. Summ. J., Ex. 7 ("Sanchez Dep.") 68:11–69:2 (characterizing the "clean[liness]" of an advertisement as "the design of [the] widget and the images that are displayed in the widget"); Alexander Decl. Supp. Defs.' Mot. Summ. J., Ex. 7 ("Houck Dep.") 40:16–18 ("What do you mean by, 'cleaner'?" / "We don't do belly-fat ads or electronic cigarette ads or work-from-home schemes."); *see also* King Dep. 71:517; Alexander Decl. Opp'n Pl.'s Mot. Summ. J., Ex. 7 ("Kane Dep.") 86:25–87:6).[FN4]

FN4. In addition, to the extent that Congoo brings a claim based on Plaintiff's failure to comply with FTC guidelines, "it is clear that no private right of action arises under [the Federal Trade Commission] Act." *Naylor v. Case & McGrath, Inc.*, 585 F.2d 557, 561 (2d Cir.1978).

***14** Further, Broadspring's representations regarding the CPM it pays publishers (*see, e.g.*, Houck Dep. 26:2–6, 39:23–40:3) were, at most, non-specific, boastful statements regarding the superiority of its product, statements that are non-actionable under unfair competition law.[FN5] *See Time Warner, Inc. v. DIRECTV, Inc.*, 497 F.3d 144, 160 (2d Cir.2007) (noting that "a general claim of superiority over comparable products that is so vague that it can be understood as nothing more than a mere expression of opinion" cannot form the basis of a false advertising claim); *Stokely–Van Camp Inc. v. Coca–Cola Co.*, 646 F.Supp.2d 510, 529–30 (S.D.N.Y.2009) (noting that a tagline was non-actionable puffery because it was "vague and non-specific"); *Julie Research Labs., Inc. v. Gen. Resistance, Inc.*, 268 N.Y.S.2d 187, 189 (1st Dep't 1966), *aff'd*, 19 N.Y.2d 906 (1967) ("The defendant's advertisements, amounting to no more than a claim in general terms of superiority of its product over the products of competitors, constitute mere 'puffing' and are not actionable."). Similarly, the statements fall far short of the degree of impropriety required for a tortious interference claim, *see Guard–Life Corp. v. Parker Hardware Mfg. Corp.*, 50 N.Y.2d 183, 189–90 (1980) (noting that "wrongful means ... do not ... include persuasion alone although it is knowingly directed at interference with the contract"); *White Plains Coat & Apron Co.*, 8 N.Y.3d at 427 ("Sending regular advertising and soliciting business in the normal course does not constitute inducement of breach of contract.").[FN6] Accordingly, Defendants' counterclaims fail as a matter of law and must be dismissed.

FN5. It is not clear that the theory of Congoo's unfair competition claim is viable in the first place. "[T]he essence of an unfair competition claim under New York law is that the defendant misappropriated the fruit of plaintiff's labors and expenditures by obtaining access to plaintiff's business idea ... through fraud or deception." *Telecom Int'l*

Am. Ltd. v. AT & T Corp., 280 F.3d 175, 197 (2d Cir.2001) (internal quotation marks omitted); *see also Eagle Comtronics v. Pico Prods.*, 682 N.Y.S.2d 505, 506 (4th Dep't 1998) ("[T]he gravamen of a claim of unfair competition is the ... misappropriation of a commercial advantage belonging to another"). Although there is some authority in this Circuit for the proposition that an unfair competition claim may be grounded in deception as well as misappropriation, *see Frink Am., Inc. v. Champion Rd. Mach. Ltd.*, 216 F.3d 1072, 2000 WL 754945, at *3 (2d Cir.2000) (summary order) (noting that a claim for unfair competition under New York law "must be grounded in *either deception or* appropriation of the exclusive property of the plaintiff" (quoting *H.L. Hayden Co. v. Siemens Med. Sys., Inc.*, 879 F.2d 1005, 1025 (2d Cir.1989)), that authority has been called into question, *see Dayton Superior Corp. v. Marjam Supply Co.*, No. 07–CV–5215 (DRH), 2011 WL 710450, at *17–18 (E.D.N.Y. Feb. 22, 2011) (noting that the quoted language from *H.L. Hayden* "did not represent the holding of the Second Circuit, but was taken from the circuit court's recitation of the legal standard applied by the district court below," and collecting cases holding that allegations of deception without misappropriation are insufficient to state a claim for unfair competition). The Court need not reach the question here, as the unfair competition counterclaim fails for independent reasons.

FN6. Neither *Curren v. Carbonic Systems, Inc.*, 872 N.Y.S.2d 240 (3d Dep't 2009), nor *Mahoney v. State of N.Y.*, 665 N.Y.S.2d 691 (3d Dep't 1997), upon which Defendants rely (Defs.' Mem. Opp'n Pl.'s Mot. Summ. J. 12), suggests otherwise. In *Curren*, the Court did not, as Congoo represents, "reverse summary judgment on [the plaintiff's] tortious interference claim" (*id.*), but rather reversed the lower court's dismissal of the plaintiff's defamation claim, and actually affirmed the dismissal of the tortious interference claim as a "repetition of his defamation claims." *Curren*, 665 N.Y.S.2d at 244. And while the *Mahoney* Court did affirm the lower court's denial of summary judgment on a tortious interference claim where allegedly false and misleading statements might have caused plaintiffs to lose a government contract, the record—unlike that here—"could arguably [have] support[ed] a finding that some of the conduct and statements ... were motivated solely by disinterested malevolence' " toward the plaintiffs. *Mahoney*, 665 N.Y.S.2d at 694.

MOTIONS TO EXCLUDE EXPERT TESTIMONY

Next, the Court addresses the dueling motions to exclude expert testimony at trial. (Docket Nos. 94, 102). Defendants have offered the expert report of Lance James in support of their motion for summary judgment, and, in rebuttal, Plaintiff has offered a report of its expert, Marty Lafferty. (*See* Pl.'s Mem. Law Supp. Mot. Strike Expert Report & Preclude Test. Lance James (Docket No. 103) (Pl.'s Exclusion Mem.), Ex. 1 ("James Report"); Decl. Martin C. Lafferty ("Lafferty Decl."), Ex. A ("Lafferty Report")). To the extent that the parties move to strike the reports themselves, their motions are moot as the Court did not rely on the reports in reaching its conclusions on their cross-motions for summary judgment. Each side, however, also moves to preclude the other side's expert from testifying at trial. As the case will now proceed to trial (absent settlement), those portions of the parties' motions are not moot.

The admissibility of expert testimony is governed by Rule 702 of the Federal Rules of Evidence, which provides, in relevant part that "[a] witness who is qualified as an expert by knowledge, skill, experience,

training, or education may testify" to his opinion if:

> (a) the expert's scientific, technical, or other specified knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
>
> ***15** (b) the testimony is based on sufficient facts or data;
>
> (c) the testimony is the product of reliable principles and methods; and
>
> (d) the expert has reliably applied the principles and methods to the facts of the case.

Fed.R.Evid. 702. In *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 597 (1993), the United States Supreme Court defined the "gatekeeping role" of district courts with respect to expert testimony, declaring that "the Rules of Evidence—especially Rule 702—[ ] assign to the trial judge the task of ensuring that an expert's testimony both rests on a reliable foundation and is relevant to the task at hand." The Rule 702 inquiry is a "flexible" one that "depends upon the particular circumstances of the particular case at issue." *Floyd v. City of New York*, 861 F.Supp.2d 274, 286 (S.D.N.Y.2012) (internal quotation marks omitted). Although a district court should "admit expert testimony only where it is offered by a qualified expert and is relevant and reliable," *Cohalan v. Genie Indus., Inc.*, 10–CV–2415 (JMF), 2013 WL 829150, *3 (S.D.N.Y. Mar. 1, 2013) (internal quotation marks omitted), exclusion remains "the exception rather than the rule," *Floyd*, 861 F.Supp.2d at 287 (internal quotation marks omitted).

A. Plaintiff's Motion To Exclude the Testimony of Lance James

The Court first addresses Plaintiff's motion to exclude the testimony of Defendants' expert, Lance James, who offers opinions on whether MindSet distributed spyware and adware during the period 2003–2005, including software titled 'FavoriteMan' and 'Netpals.' (James Report 1). Plaintiff argues that James's testimony, or at least portions of it, should be excluded, for five reasons. First, Plaintiff argues that James's testimony is irrelevant, as he has not offered any assurance that the software he analyzed was actually software that Mindset distributed. (Pl.'s Exclusion Mem. 3–4). Second, Plaintiff disputes the reliability of James's opinions, arguing that he has not explained his methodologies, and that his opinions are *ipse dixit*. (*Id.* at 4–5). Plaintiff's third argument is that James offers inadmissible opinions about the mental states of the spyware programmers. (*Id.* at 6–7). Fourth, Plaintiff claims that James's opinions improperly "introduc[e] hearsay." (*Id.* at 5–6). And finally, Plaintiff contends that James's opinions about the relationships among Broadspring, Mindset, Addictive Technologies, and Vista Interactive are improper subjects for expert testimony. (*Id.* at 7).

Plaintiff's first argument, that James's testimony is irrelevant, is plainly meritless, as James's report speaks to the truth of Defendants' allegedly defamatory statements, which is obviously at issue in this litigation. *See* Fed.R.Evid. 401. Even if Plaintiff's argument were reframed as relating to the requirement of Rule 702 of the Federal Rules of Evidence that expert testimony be "based on sufficient facts or data," Fed.R.Evid. 702(b), it would fail. In general, "[q]uestions over whether there is a sufficient factual basis for an expert's testimony may go to weight, not admissibility." *Cedar Petrochems., Inc. v. Dongbu Hannong Chem. Co., Ltd.*, 769 F.Supp.2d 269, 285 (S.D.N.Y.2011) (internal quotation marks omitted). That is certainly the case here, where James has offered supplemental testimony explaining how he verified that the files he analyzed were, in fact, "the files distributed by Mindset Interactive d/b/a Additive Technologies." (Decl. Lance James (Docket No. 128) ¶ 2(a)). Plaintiff's citation of *General Electric Co. v. Joiner*, 522 U.S. 136, 144–46 (1997), is therefore inapt, as in that case there was no dispute over what carcinogens were analyzed in the epidemiological

studies relied upon by the expert. (Pl.'s Reply Mem. Law Further Supp. Mot. Strike Expert Report & Preclude Test. Lance James) (Docket No. 155) ("Pl.'s Exclusion Reply Mem.") 3).

***16** Plaintiff's second argument is also unpersuasive. Plaintiff contends that the James Report is unreliable because it fails to explain the methodologies that James employed in conducting his analysis, rendering it impossible to subject the report to any sort of testing. (Pl.'s Exclusion Mem. 4–5). Although the James Report is far from a model of clarity, and it does not define certain terms, the Court does not agree that it contains "no method whose reliability can be tested." *Fate v. Vill. of Spring Valley*, No. 11–CV–6838 (JPO), 2013 WL 2649548, at *4 (S.D.N.Y. June 13, 2013) (internal quotation marks omitted). To the contrary, the report guides the reader through each step of the analysis and indicates which findings suggested to James that the programs behaved like spyware. (*See, e.g.*, James Report 13 ("After bass.dll was installed there was an extra executable installed ... in the system32 directory .... The only files that should be stored in this directory are system files that are installed onto the operating system by default ...."). To the extent that Plaintiff] takes issue with James's conclusions, "they may be properly explored on cross-examination and go to [the] testimony's weight and credibility—not its admissibility." *Int'l Bus. Machs. Corp. v. BCG Partners, Inc.*, No. 10–CV–128 (PAC), 2013 WL 1775437, at *16 (S.D.N.Y. Apr. 25, 2013) (alteration and internal quotation marks omitted).

Third, the Court does not agree with Plaintiff's view that James's testimony improperly opines on people's states of mind. It is true that James, at certain points in his report, uses terms such as "surreptitious" and "inconsideration." (James Report 22–23; *see also* Pl.'s Exclusion Reply Mem. 10). But the thrust of the report has nothing to do with the mental states of those who designed the alleged spyware, but rather concerns the nature of the programs analyzed. *See Arista Records LLC v. Lime Grp. LLC*, 784 F.Supp.2d 398, 414 (S.D.N.Y.2011) (finding that the challenged expert had "not opined on the parties' state of mind, but rather ha[d] provided information on the *design* and *functionality* of the LimeWire program"). Indeed, it is unclear why Defendants would even seek to admit testimony about the states of mind of Mindset's programmers, as there is no indication in the record as to who the programmers were or why their mental states would be at all relevant in this litigation. Accordingly, Plaintiff's third argument does not serve as a basis to preclude James's testimony either.

Fourth, although James does reproduce the results of Internet searches and other third-party statements in his report, that does not render all of his testimony inadmissible hearsay. Experts may not "simply transmit ... hearsay to the jury," but they are permitted to rely on hearsay if "experts in the field reasonably rely on such evidence in forming their opinions." *United States v. Mejia*, 545 F.3d 179, 197 (2d Cir.2008). An expert relying on hearsay, however, "must form his own opinions by applying his extensive experience and a reliable methodology to the inadmissible [hearsay] materials." *Id.* (internal quotation marks omitted). Here, in some portions of his report, James has relied on his specialized knowledge in the field of information security to synthesize information from his diverse sources and to form an opinion as to whether FavoriteMan or Netpals were, indeed, spyware. (*See, e.g.*, James Report 24 ("I used the following well-respected and well-known publicly available sites to conduct automated binary analysis submissions to determine detection rates from the most commonly employed Anti–Virus software ... I researched the industry standard blocklists ...."). *Cf. Marvel Characters, Inc. v. Kirby*, 726 F.3d 119, 135–36 (2d Cir.2013) (noting that a historian would be permitted to "helpfully synthesize dense or voluminous historical texts" or "offer background knowledge or context that illuminates or places in perspective past events"); *Linde v. Arab Bank, PLC*, 922 F.Supp.2d 316, 332 (E.D.N.Y.2013) (denying motion to exclude terrorism expert whose research was conducted solely

on the Internet, but who "synthesize[d] th[e] material and pull[ed] together common themes in reaching his conclusions"). In those respects, his testimony is proper and Plaintiff's motion is without merit.

***17** At other points, however, James's report crosses the line into improper regurgitation of hearsay. In particular, a substantial portion of the James Report is devoted to reproducing screenshots of archived Internet pages (James Report 31–40) in an effort to demonstrate that "Addictive Technologies was a MindSet Interactive Company in 2004, and was observed as owned by Broadspring in or about 2005," and that "Broadspring claimed ownership to Addictive Technologies and Mindset Interactive," (James Report 41). Yet the significance of those archived pages to the relationships among Broadspring, Addictive Technologies, and Mindset Interactive is made no more apparent by James's testimony. That is, as Plaintiff argues in its fifth point, that portion of James's testimony violates Rule 702's requirement that expert testimony "help the trier of fact to understand the evidence or to determine a fact in issue." Fed.R.Evid. 702(a); *see also In re Fosamax Prods. Liab. Litig.*, 645 F.Supp.2d 164, 173 (S.D.N.Y.2009) ("[E]xpert testimony is not helpful if it simply addresses lay matters which the jury is capable of understanding and deciding without the expert's help." (internal quotation marks omitted)). Put simply, James—an expert in information security—brings no expertise to bear on the legal relationships among Broadspring, Mindset, Addictive Technologies, and Vista Interactive; accordingly, he is precluded from offering any opinions regarding the relationships among them, and any archived Internet pages that Defendants seek to admit on that topic must be introduced through competent fact witnesses.

B. Defendants' Motion To Exclude the Testimony of Marty Lafferty

Turning to Defendants' motion to exclude Lafferty's testimony, Defendants offer three arguments. First, they argue that Lafferty is insufficiently qualified to testify on the subject matter of his report. (Def. Congoo's Mem. Law Supp. *Daubert* Mot. Exclude Pl.'s Purported Spyware 'Expert' (Docket No. 95) ("Defs.' Exclusion Mem.") 6–9). Second, they contend that Lafferty's opinions are inadmissible because his report improperly opines on James's credibility. (*Id.* 10–11). And third, they allege that the report contains certain clerical errors—namely, that it is unsigned, does not include a list of Lafferty's publications as required by Rule 26(a)(2)(B) of the Federal Rules of Civil Procedure, and does not include a list of cases in which Lafferty has testified, as required by that same Rule. (*Id.* 11–12).

Addressing the first argument, pursuant to Rule 702, a proffered expert must be qualified "by knowledge, skill, experience, training, or education." Fed.R.Evid. 702. "To determine whether a witness qualifies as an expert, courts compare the area in which the witness has superior knowledge, education, experience, or skill with the subject matter of the proffered testimony." *United States v. Tin Yat Chin*, 371 F.3d 31, 40 (2d Cir.2004). "The Second Circuit has taken a liberal view of the qualification requirements of Rule 702, at least to the extent that a lack of formal training does not necessarily disqualify an expert from testifying if he or she has equivalent relevant practical experience ." *In re Rezulin Prods. Liab. Litig.*, 309 F.Supp.2d 531, 559 (S.D.N.Y.2004); *see also Peerless Ins. Co. v. Marley Engineered Prods. LLC*, No. 05–CV–4848 (AKT), 2008 WL 7440158, at *2 (E.D.N.Y. June 12, 2008) ("This Circuit has adopted a liberal standard for qualifying an expert and there is no requirement that a witness have formal education or training before being qualified as an expert." (citing *Nimely v. City of New York*, 414 F.3d 381, 396 (2d Cir.2005))). "If an expert's training and experience is in a field closely related to the area to the proposed testimony, that may—in appropriate circumstances—be sufficient to meet Rule 702's qualification standards." *SEC v. Tourre*, 950 F.Supp.2d 666, 674 (S.D.N.Y.2013).

***18** In this case, Lafferty's expertise is derived from his experience as the Chief Executive Officer of the Distributed Computing Industry Association ("DCIA"), "an organization focused on fostering technological and commercial advancement of cloud computing, peer-to-peer ... software, and related technologies." (Lafferty Decl. ¶ 1). The member companies of the DCIA include software developers to whom spyware and malware represent a significant concern, and Lafferty has testified that he is "directly involved in ... find [ing] ways to eliminate and protect against 'spyware' and other types of 'malware.' " (*Id.* ¶¶ 2–3). In addition, Lafferty has served as the intermediary between federal agencies, on the one hand, and DCIA member companies, on the other, "where the subject matter was software analysis and the development of assurances that no 'malware' was present." (*Id.* ¶ 7). Perhaps most significantly, Lafferty "contributed substantially" (albeit almost a decade ago) to an FTC multi-day workshop aimed at defining the terms "spyware, malware, and adware," definitions that are still "considered to be the industry standard today." (*Id.* ¶ 8).

The Court concludes that such experience is sufficient to qualify Lafferty as an expert to opine on the James Report's claim "that Mindset Interactive Inc.... distributed spyware during the period 2003–to–2005, and in particular [that] its FavoriteMan and NetPals software applications constituted spyware." (Lafferty Report 1). Defendants argue that Lafferty is not qualified to offer an opinion on that subject because he has no "computer science background or any other relevant technical knowledge that would permit him to analyze the Mindset Software" and because his professional experience in the field is not sufficiently substantial. (Defs.' Reply Mem. Law Further Supp. *Daubert* Mot. Exclude Pl.'s Purported Spyware 'Expert' (Docket No. 152) ("Defs.' Exclusion Reply Mem.") 3–4). But, as noted, a witness need not have any formal education or training before being qualified as an expert, so long as the expert is proffering an opinion on an issue that is within his area of expertise. *Peerless*, 2008 WL 7440158, at *2; *see also McCullock v. H.B. Fuller Co.*, 61 F.3d 1038, 1043 (2d Cir.1995) (holding that disputes over expert qualifications are "properly explored on cross-examination and [go] to [the] testimony's weight and credibility—not its admissibility").

The issues in the Lafferty Report are indeed within Lafferty's area of expertise, as much of the report concerns whether certain qualities that James observed about the analyzed software are indeed characteristic of spyware, a concept with which Lafferty is intimately familiar. (*See, e.g.*, Lafferty Report 5–6 ("Contextual analysis, starting with James' Figure 1, which was provocatively labeled as 'McAfee Security Identifying NetPals as Spyware' reveals that, according to respected malware protection company Emsisoft (www.emsisoft.com), James' specifically selected file, 17odhr0b.exe, is actually a file within a program known as 'J–Ball' distributed by the company Just Free Games (www.gametopcom) a completely separate company from Mindset Interactive .... Its threat level is considered by Emsisoft as 'low risk,' and certainly not serious enough to be considered spyware."); *id.* 15 ("I respectfully disagree with James that the packing of the relatively small 17b0drhr0b.exe file 'strongly suggests that it is intended to obfuscate and hide the activity of the executable, such as surreptitiously install software that is designed to hook directly into the browser.' Rather, this can be viewed alternatively as an elegant and efficient approach to designing software that has no more sinister a purpose than to serve relevant advertising.")). Accordingly, the Court will not exclude Lafferty's testimony on those grounds.

***19** Defendants' second and third objections are even less weighty. Their argument that Lafferty's report improperly opines on James's credibility is plainly meritless. Indeed, Defendants do not seem to understand the meaning of the term "credibility," as they suggest that Lafferty's conclusion that the James Report offers "insufficient evidence to prove that the

software can reasonably be considered spyware" is somehow a challenge to James's credibility. (Defs.' Exclusion Mem. 10 (alteration, emphasis, and internal quotation marks omitted)). To the contrary, Lafferty's report quite obviously criticizes the substance of James's report, and the fact that Lafferty questions whether James analyzed the correct files does not mean that he has "opine[d] on the credibility of evidence"; his report is simply "archetypal rebuttal testimony" that "identifies a flawed premise in an expert report that casts doubt on ... that report's conclusions." *Scientific Components Corp. v. Sirenza Microdevices, Inc.*, No. 03–CV–1851 (NGG)(RML), 2008 WL 4911440, at *2 (E.D.N.Y. Nov. 13, 2008); *see also Ross Univ. Sch. Med., Ltd. v. Brooklyn–Queens Health Care, Inc.*, No. 09–CV–1410 (KAM), 2012 WL 6091570, at *7 (E.D.N.Y. Dec. 7, 2012) (describing a rebuttal report that "object[ed] to [the opposing expert's] methodology").

Finally, the Court will not exclude Lafferty's testimony because of the three technical failings that Defendants have identified. Putting aside who is to blame for those failings (*compare* Pl.'s Mem. Law. Opp'n Defs.' Mot. Exclude Expert Test. Martin C. Lafferty (Docket No. 130) ("Pl.'s Mem. Opp'n Exclusion") 6, *with* Defs.' Exclusion Reply Mem. 9), any harm incurred by Defendants as a result of those failings has been minimal, and certainly would not justify the relatively harsh sanction of exclusion. *Croom v. W. Conn. St. Univ.*, 218 F.R.D. 15, 18 (D.Conn.2002) ("The remedy of preclusion is not to be employed as a 'paper tiger' with parties capitalizing on technical mistakes in discovery, but rather should be employed sparingly when the circumstances demand such a drastic measure."). Plaintiff has remedied the signature defect, and the only incidental costs that Defendants claim to have incurred are minimal costs for "independently research[ing] information that should have been provided by Plaintiff." (Defs.' Exclusion Reply Mem. 10).[FN7] The Court is unpersuaded by that claim, not only because Defendants provide no documentation of their costs, but also because Defendants do not specify what additional information Plaintiff should have provided, particularly in light of Lafferty's testimony that he has not testified as an expert in the past four years and thus was not obligated to provide additional information about his background. (Lafferty Decl. ¶ 10). Accordingly, Defendants' motion to exclude Lafferty's testimony is denied.

FN7. Although Defendants request that the Court direct Plaintiff to pay Defendants' costs for filing the motion to exclude Lafferty's testimony because Plaintiff offers "no legitimate reason why it omitted Lafferty's signature, relevant experience and list of publications," the Court will not do so, especially because most of Defendants' motion was unrelated to those particular defects. (Defs .' Exclusion Reply Mem. 10 n. 5).

MOTIONS FOR SANCTIONS

Next, the Court addresses Plaintiff's motions for sanctions. As noted, Plaintiff makes two such motions. First, pursuant to this Court's Order of October 16, 2013 (Docket No. 60), Plaintiff moves *in camera* for re-designation of certain documents produced and designated by Defendants as AEO, as well as associated attorney's fees and costs. Second, Plaintiff moves for sanctions due to Defendants' alleged spoliation of evidence—namely, the failure to preserve certain Instant Messages ("IMs"). (Docket No. 98).

A. The Re–Designation Motion

***20** Plaintiff's first motion is based on the Confidentiality Stipulation and Protective Order (the "Protective Order"), which was so ordered by the Court on May 17, 2013. (Docket No. 34). The Order provides for two levels of confidentiality: documents designated "Confidential," which may be shared with clients for use only in connection with this litigation; and documents designated "Highly Confidential—Attorneys' Eyes Only," which may be viewed only by the parties' outside counsel of record in this

case (and by certain experts and others). (*Id.* §§ 2.3, 2.4, 7.2, 7.4). By its terms, the Protective Order strictly limits the latter designation to "extremely sensitive Confidential Information or Items whose disclosure to another Party or nonparty would create a substantial risk of serious injury that could not be avoided by less restrictive means." (*Id.* § 2.4). In addition, the Protective Order provides that the designating party "must take care to limit any such designation to specific material that qualifies under the appropriate standards," and "to designate for protection only those parts of ... documents ... that qualify." (*Id.* § 5.1). Significantly, in the event of a dispute over any designations, the Protective Order imposes the "burden of persuasion ... on the Designating Party." (*Id.* § 6.3). Moreover, the Protective Order expressly provides that "[d]esignations that are shown to be clearly unjustified, or that have been made for an improper purpose (e.g., to unnecessarily encumber or retard the case development process, or to impose unnecessary expenses and burdens on other parties), may expose the Designating Party to sanctions." (*Id.* § 5.1).

On October 7, 2013, Plaintiff filed a letter motion requesting a conference regarding, *inter alia*, Defendants' alleged misuse of the AEO designation. (Docket No. 53). Notably, this was not the first time that Plaintiff had raised the issue; on July 19, 2013, Plaintiff protested Defendants' designation of certain documents as AEO (Docket No. 42), in response to which Defendants voluntarily removed the AEO designation on some of those documents (Docket No. 41).[FN8] Prompted by Plaintiff's October 7, 2013 letter, the Court held a conference on October 16, 2013. (Docket No. 60). At the conference, Defendants admitted that they had continued to inappropriately mark certain documents AEO, and that they would re-designate those documents accordingly. (Docket No. 67, at 6:20–22). That same day, the Court issued an Order directing Defendants to review all documents they had designated as AEO, and to re- or de-designate any such documents as appropriate by October 23, 2013. (Docket No. 60). In the event that Plaintiff believed that documents remained improperly designated AEO, Plaintiff was to submit the relevant documents to the Court for *in camera* review. (*Id.*). The Court cautioned Defendants that "[i]f there is a single line that is properly designated AEO," that would not justify "withhold[ing] the entire document as AEO." (Docket No. 67, at 11:14–16). More significantly, the Court explicitly warned that if it disagreed with Defendants' designations, "there [would] be consequences," including "whatever fees [Plaintiff has] incurred in order to address the issue, including whatever motion practice is necessary in connection with this." (*Id.* at 9:4–8).

> FN8. Defendants re-designated and re-produced documents that had been improperly designated AEO on other occasions, without Court intervention. Defendants themselves admit that, in total, they re-designated and re-produced documents on nine separate occasions between July and October 2013. (Defs.' Mem. Opp'n Pl.'s Mot. Re–Designation Documents & Sanctions ("Defs.' Re–Designation Opp'n Mem.") 2 n. 1).

***21** Remarkably, as a result of that court-ordered review, Defendants re-designated an additional 780 documents, effectively conceding that a large number of their designations—even after multiple rounds of review—had been improper. (Pl.'s Mem. Law Supp. Re–Designation Defs.' Documents & Sanctions ("Pl.'s Re–Designation Mem.") 2; Defs.' Re–Designation Opp'n Mem. 2). More than 1,000 documents allegedly remain designated AEO (Defs.' Re–Designation Opp'n Mem. 2), of which Plaintiff now challenges approximately nineteen (totaling approximately fifty-eight pages).[FN9] Having reviewed those documents, and the parties' respective memoranda, the Court concludes that many of the documents at issue remain improperly designated AEO. For instance, Defendants designated AEO an entire e-mail thread among Con-

goo employees discussing their concerns about publishers that were "dropping like flies." (C00007052–7054). Only small excerpts from these e-mails—specifically, the portions discussing the terms of Congoo's agreements with publishers (*see, e.g.*, C00007053 (stating the notice period for termination of certain accounts))—could even plausibly be construed as containing "extremely sensitive" information, but Defendants designated the whole thread AEO. Notably, Defendants all but admitted that such a blanket designation was improper, stating in their memorandum that "[m]ultiple numbers and sentences would need to be redacted to re-designate" the document. (Defs.' Re–Designation Opp'n Mem. 4).

> FN9. Plaintiff suggests that the number of improperly designated documents is significantly higher, but alleges that it has focused its motion on a subset of more significant documents so as "not to burden the Court." (Pl.'s Re–Designation Mem. 3). Some of the documents challenged by Plaintiff in its initial memorandum—namely, C00010997, C00007393–94, and C0001400508 (*id.* at 4)—are no longer at issue. In conjunction with their opposition, Defendants redesignated and re-produced C0010997, explaining that they had inadvertently failed to produce it earlier; Defendants had previously re-designated the other documents—a fact inadvertently overlooked by Plaintiff. (Defs.' Re–Designation Opp'n Mem 6 & n. 3).

Defendants make a similar admission with respect to an e-mail from Cosentino notifying Reader's Digest that it was in breach of its agreement, acknowledging that the document could be re-designated confidential so long as "[m]ultiple sentences" were redacted. (Defs.' Re–Designation Opp'n Mem. 4; *see also* C00013447). In the Court's judgment, even that admission does not go far enough. There is arguably one contractual term in the e-mail that could be considered sensitive and justify redaction (namely, the penultimate sentence of the second paragraph of text), but that does not justify designating "[m]ultiple sentences," let alone the entire e-mail, AEO. To provide just one more example: Plaintiff points to a document displaying two screenshots—one from a Congoo website and the other from a Broadspring website—where the text that compares the appearance of the two images was redacted as AEO. (Pl.'s Re–Designation Mem. 6; *see also* C00008758). It strains credulity to assert, as Defendants do, that that text is "extremely sensitive" information; it is certainly not, as Defendants assert, "internal strategy and analysis of competition" that would justify an AEO designation. (Defs.' Re–Designation Opp'n Mem. 7).

More broadly, putting aside isolated references in the documents at issue to the terms of agreements with customers and the like, Defendants fail to carry their burden of persuasion that any of the designations at issue are proper. (Indeed, they fail even to acknowledge that it is their burden, taking Plaintiff to task for allegedly failing to show that disclosure of the documents at issue would not harm them. (Defs.' Re–Designation Opp'n Mem. 5).) Over and over again, Defendants merely assert, in conclusory fashion, that the designations and redactions at issue are proper because the information concerns "client acquisition strategy," "client retention strategy," "internal strategy and analysis of competition," "client descriptions," or "terms of its client agreement." (*See, e.g., id.* at 4, 7). Such perfunctory explanations, however, fall far short of satisfying Defendants' burden of showing that disclosure of the redacted material "would create a *substantial* risk of serious injury that could not be avoided by less restrictive means." (Protective Order § 2.4 (emphasis added)).

***22** Accordingly, to the extent that Defendants have not already done so, they are ORDERED to re-designate as Confidential and re-produce to Plaintiff the following documents within **one week** of the date of this Opinion and Order: C00013033–38, C00013436, C00013447–48, C00014365–66,

C00014377–79, C00007207, C00014396–99, C00014781–82, C00007052–54, C00002131–43, C00006889–91, and C00011149–54. If Defendants believe that redactions to those documents are justifiable, they may make such redactions, subject to the understanding that Plaintiff may challenge the redactions and mindful that the Court is unlikely to approve redactions that go beyond specific references to contractual terms, rates (including but not limited to CPM information), and performance references. Moreover, Defendants are cautioned that, in the event that the redactions are found to be improper, they may be ordered to pay the attorney's fees and costs associated with that additional litigation. If Defendants make such redactions, any challenges by Plaintiff to the redactions shall be made to the Court within **two weeks** of the date of this Opinion and Order, and Defendants' reply, if any, shall be made within **three weeks** of the date of this Opinion and Order. Additionally, Defendants are ORDERED to re-designate the redactions on the following documents from AEO to Confidential and to reproduce the documents to Plaintiff within **one week** of the date of this Opinion and Order: C00008156, C00008758, C00008680, C00000383, and C00011121.

Pursuant to the terms of the Protective Order, as well as the Court's inherent authority under Rule 37 of the Federal Rules of Civil Procedure, Plaintiff is also entitled to reasonable attorney's fees and costs incurred as a result of Defendants' improper AEO designations, including the fees and costs associated with bringing this motion for sanctions. (Protective Order § 5.1 ("Designations that are shown to be clearly unjustified ... may expose the Designating Party to sanctions.")). *See Del Campo v. Am. Corrective Counseling Servs., Inc.*, No. 01–CV–21151 (PVT), 2007 WL 3306496, at *4 (N.D.Cal. Nov. 6, 2007) ("The failure to obey a protective order's prohibition against indiscriminate designations is covered by Rule 37."); *In re ULLICO Inc. Litig.*, 237 F.R.D. 314, 317–19 (D.D.C.2006) (ordering a party to pay its opponent's expenses and fees incurred in filing a successful motion challenging the over-designation of documents as confidential). The fact that Defendants' designations were "clearly unjustified," by itself, warrants the imposition of sanctions under the Protective Order. (Protective Order § 5.1). Sanctions are even more appropriate in view of Defendants' abuse of the AEO designation throughout the discovery process. As noted above, Defendants redesignated and re-produced documents on nine separate occasions—including, most notably, 780 documents that were re-designated only after evidence of some patently improper designations prompted the Court, on Plaintiff's application, to order Defendants to engage in a wholesale review of all documents it had designated AEO. Plaintiff shall submit its application for reasonable costs and fees, with supporting contemporaneous documentation, within **two weeks** of the date of this Opinion and Order. Defendants must submit any opposition within **three weeks** of the date of this Opinion and Order.

***23** Finally, although the Court recognizes that the documents at issue are confidential and are thus not appropriate to be placed in the public record, it sees no reason why the memoranda of law the parties filed in support of and in opposition to the instant re-designation motion should remain under seal, as the memoranda appear to contain only general descriptions of the documents rather than the confidential information itself. As those memoranda are "relevant to the performance of the judicial function and useful in the judicial process," they qualify as "judicial documents" to which the common law right of public access attaches. *Lugosch v. Pyramid Co. of Onondaga*, 435 F.3d 110, 119 (2d Cir.2006) (internal quotation marks omitted). Accordingly, the parties are ordered to show cause in writing, within **two weeks** of the date of this Opinion and Order, why their memoranda of law with respect to this motion should remain under seal or in redacted form. Any replies shall be filed within **three weeks** of the date of this Opinion and Order. In the absence of a showing that the memoranda of law should remain under seal, the parties

shall promptly file them on ECF. The Clerk of Court is directed to file and maintain the documents at issue under seal pending further order of the Court.

B. The Spoliation Motion

Plaintiff's second motion for sanctions is based on Defendants' alleged spoliation of evidence. (Docket No. 98). In particular, it is based on Defendants' October 2, 2013 admission that Congoo custodians Rafael Cosentino, Ian Kane, and Jack Wagner had not been preserving IMs sent from their Yahoo! IM accounts, in violation of this Court's Stipulation and Order for the Preservation of Documents (the "Preservation Order"), entered on March 25, 2013. (Katz Decl. Supp. Pl.'s Mot. for Sanctions (Docket No. 101), Ex. 8; Pl.'s Mem. Supp. Mot. Sanctions (Docket No. 99); *see also* Docket Nos. 10, 24). In addition to attorney's fees and expenses, Plaintiff requests that the Court give an adverse inference jury instruction because of Defendants' misconduct. (Pl.'s Mem. Supp. Mot. Sanctions 1).

"Spoliation is the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." *Cohalan*, 2013 WL 829150, at *8 (internal quotation marks omitted). "[A] party seeking an adverse inference instruction based on the destruction of evidence must establish (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a culpable state of mind; and (3) that the destroyed evidence was relevant to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense ." *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 106 (2d Cir.2002) (internal quotation marks omitted). The burden of establishing those elements falls on the party seeking sanctions—here, Plaintiff. *Byrnie v. Town of Cromwell*, 243 F.3d 93, 109 (2d Cir.2001). "The determination of an appropriate sanction for spoliation, if any, is confined to the sound discretion of the trial judge, and is assessed on a case-by-case basis." *Shrenuj USA, LLC v. Rosenthal & Rosenthal, Inc.*, No. 12–CV–4827 (JMF), 2014 WL 1226469, at *7 (S.D.N.Y. Mar. 25, 2014) (internal quotation marks omitted); *see also Valentini v. Citigroup, Inc.*, No. 11–CV–1355 (JMF), 2013 WL 4407065, at *2 (S.D.N.Y. Aug. 16, 2013) (noting the district court's "broad discretion" to fashion appropriate sanctions for discovery violations).

***24** With respect to the first element, there is no question that Defendants were under an obligation to preserve the IMs at issue. The Court's Preservation Order explicitly required the preservation of "[a]ll ... instant messaging ... related to this dispute" (Docket No. 10, ¶ 2(c)), and Plaintiff has adduced substantial evidence showing that Congoo employees use their Yahoo! IM accounts extensively for work-related purposes and that some such Yahoo! IMs are relevant to this lawsuit. (*See, e.g.*, Katz Decl. Supp. Pl.'s Mot. for Sanctions, Ex. 10 ("Kane Dep. II") 146:7–13 (Kane testifying that most Congoo employees, including everyone in business development, is required to use Yahoo! Instant Messenger); Katz Decl. Supp. Pl.'s Mot. for Sanctions, Ex. 15 (IM from Cosentino to Nashed containing the URL of the Lens)).

Turning to the second element, the Court finds that Defendants acted with gross negligence. Defendants' counsel represented to the Court on April 9, 2013, that they and Nashed were aware of the terms of the Preservation Order (Docket No. 56, at 15:9–12), and even indicated that Nashed had advised "Mr. [K]ane and Mr. Cosentino to not delete, remove anything from their computers," and that "[Nashed] went and spoke to them, personally, to ensure that no information relevant to this case would be deleted," (*id.* at 15:22–16:2). Yet the record makes clear that, in reality, Nashed failed to ensure that Kane and Cosentino understood their obligations under the Preservation Order, which required Defendants to take "all reasonable steps to preserve and retain" all electronically stored information. (Docket No. 10, § 1). Remarkably, Cosentino admitted at his deposition that he

did not even consider that his preservation obligations required him to take steps regarding his Yahoo! IM account, and he did not investigate whether the settings on his account—or any other account at Congoo—should have been changed until months after this case commenced. (Cosentino Dep. 21:3–12, 22:13–22, 23:4–14). Likewise, Kane testified that he "never looked into" whether his IMs were being preserved because it was "never really important to [him]." (Kane Dep. II, 147:21–148:9). Although the Court is not persuaded that Defendants' failures were a "conscious decision" (Pl.'s Mem. Supp. Mot. Sanctions 10), their cavalier attitude toward their preservation obligations is inexcusable. *See Orbit One Commc'ns, Inc. v. Numerex Corp.*, 271 F.R.D. 429, 441 (S.D.N.Y.2010) ("[A]fter a discovery duty is well established, the failure to adhere to contemporary standards can be considered gross negligence." (internal quotation marks omitted)).

Plaintiff has failed, however, to carry its burden with respect to the third element. Where the destruction of evidence is found to be willful, courts presume the relevance of the destroyed evidence, *see Sekisui Am. Corp. v. Hart*, 945 F.Supp.2d 494, 504 (S.D.N.Y.2013), but where the party against whom sanctions are sought engages only in gross negligence, a court may, but is not required to, presume the relevance of the evidence, *see Chin v. Port Auth. of N.Y. & N.J.*, 685 F.3d 135, 162 (2d Cir.2012) ("[A] finding of gross negligence merely permits, rather than requires, a district court to give an adverse inference instruction."); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 221 (S.D.N.Y.2003) ("[O]nly in the case of *willful* spoliation is the spoliator's mental culpability itself evidence of the relevance of the documents destroyed."). Here, Plaintiff has not submitted independent proof of the IMs' relevance; instead, it simply argues that because other IMs that were produced were favorable to its case, and because Defendants regularly use IMs to communicate about work-related matters, the unrecorded IMs must have been favorable to its case as well. (*See* Pl.'s Mem. Supp. Mot. Sanctions 8–10, 12). Without either direct proof or evidence suggesting that Defendants' conduct was willful, however, the Court declines to impose the "severe" sanction of an adverse inference. *Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC*, 685 F.Supp.2d 456, 467 (S.D.N.Y.2010); *see also Passlogix, Inc. v. 2FA Tech., LLC*, 708 F.Supp.2d 378, 415 (S.D.N.Y.2010) ("[T]he Court holds that although [Defendant] had a duty to preserve the [disputed e-mail] and was grossly negligent in deleting it, it did not engage in spoliation of evidence because [Plaintiff] has failed to establish that the e[-]mail would have been helpful to its claims or defenses or harmful to [Defendant's] claims or defenses."); *Zubulake*, 220 F.R.D. at 221–222 (declining to give an adverse inference instruction where it had not been proved that backup tapes lost by a "negligent—and possibly reckless"—party were relevant).

***25** Nevertheless, the Court still finds Defendants' conduct—particularly in light of Cosentino's and Kane's admitted failures to investigate whether their IM accounts were capable of recording or did, in fact, record messages—sanctionable. Accordingly, Defendants are ordered to reimburse Plaintiff for the fees and expenses it incurred in pursuing Cosentino's, Kane's, and Wagner's IMs, as well as for the fees and expenses incurred in prosecuting this motion for sanctions. *See, e.g., Toussie v. Cnty. of Suffolk*, No. 01–CV–6716 (JS)(ARL), 2007 WL 4565160, at *9–10 (E.D.N.Y. Dec. 21, 2007) (finding an adverse inference instruction unwarranted, but awarding costs to moving party). Plaintiff shall submit its application for reasonable costs and fees (jointly with its application for fees and costs associated with the re-designation motion), with supporting contemporaneous documentation, within **two weeks** of the date of this Opinion and Order. Defendants must submit any opposition (jointly with its opposition to any application for fees and costs associated with the re-designation motion) within **three weeks** of the date of this Opinion and Order.

MOTION FOR LEAVE TO AMEND

Finally, the Court addresses Plaintiff's motion for leave to file a Second Amended Complaint. (Docket No. 75). Under Rule 15 of the Federal Rules of Civil Procedure, "a party may amend its pleading only with the opposing party's written consent or the court's leave. The court should freely give leave when justice so requires." Fed.R.Civ.P. 15(a)(2). Because Plaintiff moves to amend after a court-ordered deadline (*see* Docket No. 25), however, Plaintiff must also demonstrate "good cause" for the amendment. Fed.R.Civ.P. 16(b)(4). [FN10] " 'Good cause' depends on the diligence of the moving party." *Parker v. Columbia Pictures Indus.*, 204 F.3d 326, 340 (2d Cir.2000). Specifically, the moving party "must demonstrate that it has been diligent in its efforts to meet the Court's deadlines," and that "despite its having exercised diligence, the applicable deadline could not have been reasonably met." *Sokol Holdings v. BMD Munai, Inc.*, No. 05–CV–3749 (DF), 2009 WL 2524611, at *7 (S.D.N.Y. Aug. 14, 2009). "A party fails to show good cause when the proposed amendment rests on information that the party knew, or should have known, in advance of the deadline." *Perfect Pearl Co., Inc. v. Majestic Pearl & Stone, Inc.*, 889 F.Supp.2d 453, 457 (S.D.N.Y.2012) (internal quotation marks omitted). Finally, leave to amend "may properly be denied for ... undue prejudice to the opposing party by virtue of allowance of the amendment." *Ruotolo v. City of New York*, 514 F.3d 184, 191 (2d Cir.2008) (internal quotation marks omitted).

> FN10. Pointing to this Court's standard Case Management Plan, which was entered on April 9, 2013 (Docket No. 25), Defendants contend that Plaintiff has to meet an even higher standard—showing "exceptional circumstances"—to amend at this point. (Defs.' Mem. Law Opp'n Pl.'s Mot. To Amend (Docket No. 82) 2–3). That contention rests on a blatant misreading of the Case Management Plan, which specifies that "[a]bsent exceptional circumstances," the *deadline* for filing motions to amend (after which the "good cause" standard applies) may not be "more than thirty ... days following the initial pretrial conference." (Docket No. 25 ¶ 4 (emphasis omitted)). That is, the "exceptional circumstances" language limits the parties' freedom to select a deadline; it has nothing to do with the standard to be applied to motions for leave to amend.

In this case, the Second Amended Complaint does not add any new causes of action; instead, it simply provides more detailed factual allegations regarding both the role that Nashed played in disseminating the Lens and Defendants' alleged continued dissemination of the Lens after the commencement of this action. (Pl.'s Mem. Law Supp. Mot. To Amend (Docket No. 77) 2–3). Moreover, it is clear that Plaintiff acted diligently in seeking leave to file an amended complaint, and could not have filed the Second Amended Complaint by the May 14, 2013 deadline to file amended pleadings. In fact, Defendants did not even make their first document production—a production of only 116 pages—until June 2013 (Katz Decl. Supp. Mot. To Amend (Docket No. 76) ¶ 3), and Plaintiff's counsel repeatedly contacted Defendants' counsel and the Court regarding the status of Defendants' document productions in the following months (*id.* ¶¶ 4–11). Defendants did not make their next production until August 21, 2013 (*id.* ¶ 8), a production that Defendants subsequently acknowledged was missing documents, including e-mails from Nashed and Cosentino (*id.*, Ex. 12). In September and October 2013, Defendants made a series of final supplemental productions, totaling nearly 10,000 additional documents, or eighty percent of the total documents they produced in this case. (Katz Decl. Supp. Mot. To Amend ¶ 11). As Plaintiff comprehensively documents, most of the new factual allegations in the Second Amended Complaint are based on documents contained in those final supplemental productions. (Pl.'s Mem. Law Supp. Mot. To Amend 12–13). [FN11] Accordingly, Plaintiff easily establishes good cause to file the

Second Amended Complaint.

> FN11. Defendants argue that any new allegations based on documents produced by Defendants on October 11, 2013, are a result of Plaintiff's wrongful behavior. The October 11th production consisted of documents dated after March 19, 2013, and Defendants contend that Plaintiff initially agreed to a March 19, 2013 cut-off date for document production, but then later rescinded that agreement, at which point Defendants made the production. (Defs.' Mem. Law Opp'n Pl.'s Mot. To Amend 5, 9–10). Having reviewed the relevant correspondence, however, the Court cannot conclude that Plaintiff agreed to such a cut-off date. The negotiations over the date range appear to have been over the *start* date—rather than end date—for document production. (*See* Zimmerman Decl. Opp'n Mot. To Amend (Docket No. 83), Ex. 2 ("[P]lease explain precisely which of the document you requests you propose to limit to March 20, 2012 *through the present.*" (emphasis added))). Defendants' argument that they understood Plaintiff to have agreed to such a cut-off is also undermined by the fact that they produced documents dated after March 19, 2013, well after the agreement is alleged to have been reached. (*See* Katz Reply Decl. Supp. Mot. To Amend (Docket No. 87), Ex. 22).

***26** Having concluded that Plaintiff has shown good cause, the burden is on Defendants to demonstrate that the proposed amendment would be prejudicial. *See Amaya v. Roadhouse Brick Oven Pizza, Inc.*, 285 F.R.D. 251, 253 (E.D.N.Y.2012). Defendants have not done so. First, Defendants' argument that they will be hindered in their ability to prepare their motion for summary judgment is now moot, as Defendants already filed their motion for summary judgment and the Court has denied it (based on the First Amended Complaint). (*See* Defs.' Mem. Law Opp'n Pl.'s Mot. To Amend 12–13). In addition, the Court rejects Defendants' argument that they need additional discovery to respond to the Second Amended Complaint. (*See id.* 13–14). This is not a case, such as *Colon v. Southern New England Telephone Co.*, No. 09–CV–0802 (CSH), 2012 WL 6568444, at *1–3 (D.Conn. Dec. 17, 2012), where the plaintiff seeks to add entirely new causes of action to the complaint. *See also Bruce Lee Enters., LLC v. A.V.E.L.A., Inc.*, No. 10–CV–2333 (KMW), 2013 WL 364210 (S.D.N.Y. Jan. 30, 2013) (denying motion to amend where defendants sought leave to add new affirmative defenses to their answer). Instead, the Second Amended Complaint merely adds factual detail to support the existing causes of action in the Amended Complaint—detail that, it is worth noting, is derived entirely from Defendants' own document production and deposition testimony. Defendants cannot plausibly argue that they "conducted discovery without knowing that these ... allegations were at issue." *Colon*, 2012 WL 6568444, at *3; *see also In re Pfizer Inc. Sec. Litig.*, Nos. 04–CV–9866 (LTS) et al. 2012 WL 983548, at *2 (S.D.N.Y. Mar. 22, 2012) ("Courts routinely grant leave to amend when a plaintiff seeks to refine the complaint to reflect evidence obtained during discovery."). Accordingly, Plaintiff's motion seeking leave to amend the complaint is GRANTED.[FN12]

> FN12. For the same reasons, Defendants' request that discovery be reopened in the event that the Court grants Plaintiff leave to file the Second Amended Complant is denied. (Defs.' Mem. Law Opp'n Pl.'s Mot. To Amend 14–16).

The Second Amended Complaint submitted by Plaintiff includes certain redactions. By letter filed under seal dated November 13, 2013, Plaintiff indicated to the Court that the reason that it had filed a redacted version was that the Second Amended Complaint referenced discovery materials that De-

fendants had designated AEO or Confidential, pursuant to the Protective Order. In that same letter, Plaintiff stated that it did not, however, believe that any of the redacted content met the standard for being filed under seal. Now that the Court has granted Plaintiff's motion to file the Second Amended Complaint, if Defendants still intend to oppose the filing of the Second Amended Complaint in unredacted form, they must submit a memorandum, not to exceed ten pages, within **one week** of the date of this Opinion and Order, explaining why the redactions are consistent with the presumption of public access to judicial documents. *See Lugosch*, 435 F.3d at 119. Plaintiff may submit an opposition memorandum, also not to exceed ten pages, within **three weeks** of the date of this Opinion and Order. If Defendants do not oppose the filing of the Second Amended Complaint in unredacted form within **one week** of the date of this Opinion and Order, Plaintiff shall promptly file an unredacted version of the Second Amended Complaint on ECF.

SEALED DOCUMENTS

***27** In addition to the Second Amended Complaint, many of the documents upon which the Court has relied in rendering this decision were filed under seal or in redacted form. Those documents are listed in the Appendix that follows this Opinion and Order. As noted, filings that are "relevant to the performance of the judicial function and useful in the judicial process" are considered "judicial documents," to which the common law right of public access attaches. *Lugosch*, 435 F.3d at 119 (internal quotation marks omitted). Accordingly, the parties are ORDERED to show cause, in writing, why the listed documents should remain filed under seal or in redacted form, within **two weeks** of the date of this Opinion and Order. Any replies shall be filed within **three weeks** of the date of this Opinion and Order. If, within two weeks, neither party makes a filing arguing why a particular document should remain under seal, Plaintiff shall promptly file the relevant document on ECF in unredacted form.

CONCLUSION

For the reasons stated above, Defendants' motion for summary judgment is denied except with respect to the tortious interference claim against Defendant Nashed, Plaintiff's motion for summary judgment is granted, Plaintiff's motion to exclude James's testimony is granted in part and denied in part, Defendants' motion to exclude Lafferty's testimony is denied, Plaintiff's motion for sanctions based on improper AEO designations is granted, Plaintiff's motion for sanctions based on spoliation of evidence is granted in part and denied in part, and Plaintiff's motion for leave to file a Second Amended Complaint is granted. As a result of those rulings, the only remaining claims are Plaintiff's claims against Congoo, Nashed, and Cosentino under the Lanham Act and for defamation, and against Congoo and Cosentino for tortious interference.

As noted above, within **one week** of the date of this Opinion and Order, Defendants must submit any opposition to the filing of the Second Amended Complaint in unredacted form, in a memorandum not to exceed ten pages. By that same date, Defendants must also re-designate the above-referenced documents and produce them to Plaintiffs. Within **two weeks** of the date of this Opinion and Order, (1) Plaintiff must submit any challenges to redactions that Defendants make to the re-designated documents; (2) Plaintiff must submit a consolidated application for costs and fees related to the re-designation motion and the spoliation motion; and (3) either party must submit any opposition to the public filing of a document listed in the Appendix to this Opinion and Order, including the memoranda filed in support of and in opposition to the re-designation motion. Within **three weeks** of the date of this Opinion and Order, (1) Defendants may submit any reply to Plaintiff's challenges to redactions to the re-designated documents; (2) Defendants may submit any opposition to Plaintiff's application for costs and fees; (3) either party may submit a reply regarding the public filing of a document listed in the

Appendix, to the extent that any opposition has been submitted in the first place; and (4) Plaintiff may submit a reply to any opposition Defendants submit to the unredacted filing of the Second Amended Complaint, in a memorandum not to exceed ten pages.

***28** Under the Case Management Plan and Scheduling Order (Docket No. 13), the parties' Joint Pretrial Order and all related filings required by the Court's Individual Rules and Practices for Civil Cases are due thirty days from the date of this Opinion and Order. In light of the quantity and nature of the submissions that the parties need to make in the coming weeks, however, the Court will grant the parties **forty-five days from today,** rather than thirty, to make those submissions. The parties should be prepared to go to trial approximately two weeks thereafter. Moreover, the parties shall immediately advise the Court by joint letter if they are interested in a referral to the assigned Magistrate Judge for purposes of settlement.

The Clerk of Court is directed to terminate Docket Nos. 75, 94, 97, 98, 102, and 108.

SO ORDERED.

APPENDIX

The Court relied on the following documents, which were filed in redacted form, in rendering this Opinion and Order:

• Docket No. 77 (Plaintiff's Memorandum of Law in Support of its Motion for Leave to File a Second Amended Complaint)

• Docket No. 82 (Defendants' Memorandum in Opposition to Plaintiff's Motion for Leave to File a Second Amended Complaint)

• Docket No. 86 (Plaintiff's Reply Memorandum in Further Support of its Motion for Leave to File a Second Amended Complaint)

• Docket No. 100 (Defendants' Memorandum of Law in Support of Their Motion for Summary Judgment: (I) Dismissing Plaintiff's Claims for Defamation, False Advertising and Tortious Interference; and (II) Granting Defendant Congoo, LLC's Counterclaim for Unfair Competition)

• Docket No. 104 (Declaration of Ashraf Nashed)

• Docket No. 105 (Declaration of Rafael Cosentino)

• Docket No. 129 (Defendants' Memorandum in Opposition to Plaintiff's Motion for Sanctions Due to Alleged Spoliation of Evidence)

• Docket No. 136 (Defendant Congoo, LLC's Memorandum in Opposition to Plaintiff's Motion for Summary Judgment Or, Alternatively, Judgment On The Pleadings)

• Docket No. 138 (Defendant Congoo, LLC's Counterstatement of Disputed Facts Pursuant to Local Civil Rule 56.1)

• Docket No. 140 (Plaintiff's Memorandum of Law in Opposition to Defendants' Motion for Summary Judgment)

• Docket No. 141 (Declaration of Jonathan Markiles in Opposition to Defendants' Motion for Summary Judgment)

• Docket No. 144 (Plaintiff's Response to Defendants' Local Rule 56.1 Statement of Material Facts Not in Dispute)

• Docket No. 153 (Plaintiff's Reply Memorandum of Law in Further Support of its Motion for Sanctions

Due to Spoliation of Evidence)

• Docket No. 158 (Defendants' Reply Memorandum of Law in Further Support of Their Motion for Summary Judgment (I) Dismissing Plaintiff's Claims for Defamation, False Advertising and Tortious Interference and (II) Granting Defendant Congoo, LLC's Counterclaim For Unfair Competition)

The Court relied on the following documents, which were filed under seal, in rendering this Opinion and Order:

***29** • Docket No. 101, Ex. 10

• Docket No. 101, Ex. 15

• Docket No. 111, Ex. 3

• Docket No. 111, Ex. 40

• Docket No. 111, Ex. 41

• Docket No. 111, Ex. 7

• Docket No. 111, Ex. 8

• Docket No. 137, Ex. 7

• Docket No. 137, Ex. 8

• Docket No. 143, Ex. 11

• Docket No. 143, Ex. 12

• Docket No. 143, Ex. 13

• Docket No. 143, Ex. 14

• Docket No. 143, Ex. 18

• Docket No. 143, Ex. 19

• Docket No. 143, Ex. 32

• Docket No. 143, Ex. 5

• Docket No. 143, Ex. 6

• Docket No. 143, Ex. 7

• Docket No. 143, Ex. 8

• Plaintiff's Memorandum of Law in Support of Re–Designation of Defendants' Documents and Sanctions (reviewed *in camera*)

• Defendants' Memorandum in Opposition to Plaintiff's Motion for Re–Designation of Documents and Sanctions (reviewed *in camera*)

• Plaintiff's Reply Memorandum of Law in Further Support of Re–Designation of Defendants' Documents and Sanctions (reviewed *in camera*)

S.D.N.Y.,2014.
Broadspring, Inc. v. Congoo, LLC
Slip Copy, 2014 WL 4100615 (S.D.N.Y.)

END OF DOCUMENT

--- F.Supp.2d ----, 2014 WL 171599 (D.Puerto Rico)
(Cite as: 2014 WL 171599 (D.Puerto Rico))

H

Only the Westlaw citation is currently available.

United States District Court,
D. Puerto Rico.
Claudio Polo CALDERON and Jonathan Polo Echevarria, Plaintiffs,
v.
CORPORACION PUERTORRIQUE A DE SALUD and Joaquin Rodriguez–Benitez, Defendants.

Civil No. 12–1006 (FAB).
Jan. 16, 2014.

Background: Employees brought action against employer and its president, asserting discrimination claims under Title VII. Defendants filed motion in limine for exclusion of all text messages sent and received between employee and a third-party.

Holdings: The District Court, Besosa, J., held that:
(1) subpoena issued to plaintiff's cellphone carrier would not be quashed as procedurally defective;
(2) plaintiff engaged in spoliation of evidence; and
(3) adverse inference jury instruction was appropriate sanction for plaintiff's spoliation.

Motion granted in part and denied in part.

West Headnotes

[1] Witnesses 410 16

410 Witnesses
410I In General
410k16 k. Subpoena Duces Tecum. Most Cited Cases

In employment discrimination action, defendants' failure to give pre-service notice of subpoena issued to plaintiff's cellphone carrier did not warrant quashing the subpoena as procedurally defective, where, if the subpoena were quashed, it would be reissued, resulting in inefficiency, delay, and undue costs on the litigants, and defendants' late disclosure of the cellphone records did not prejudice plaintiffs. Fed.Rules Civ.Proc.Rule 45, 28 U.S.C.A.

[2] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In General. Most Cited Cases

In employment discrimination action, plaintiff engaged in spoliation of evidence, where plaintiff reasonably foresaw litigation, his texts and messages with defendant and a third-party were relevant to the lawsuit, and, while he saved those texts and messages he thought would benefit him, he did not save texts and messages that he thought would not help his side of the case.

[3] Federal Civil Procedure 170A 1551

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Doc-

uments and Other Tangible Things
170AX(E)1 In General
170Ak1551 k. In General. Most Cited Cases

Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In General. Most Cited Cases

A party has a general duty to preserve relevant evidence once it has notice of or reasonably foresees litigation; failure to preserve the evidence constitutes spoliation.

[4] Federal Civil Procedure 170A 1551

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)1 In General
170Ak1551 k. In General. Most Cited Cases

The duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation.

[5] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In General. Most Cited Cases

Federal Civil Procedure 170A 2173

170A Federal Civil Procedure
170AXV Trial
170AXV(G) Instructions
170Ak2173 k. Necessity and Subject Matter. Most Cited Cases

Adverse inference jury instruction, rather than dismissal of entire lawsuit, was appropriate sanction for plaintiff's spoliation of evidence, in employment discrimination action, where plaintiff knew of both potential for litigation and potential relevance of unsaved texts and messages, and his failure to preserve texts and messages he felt would not support his case severely prejudiced defendants by precluding a complete review of conversations and pictures sent between plaintiff and a third-party, and prevented defendants from introducing other writings that in fairness ought to be considered at same time as messages that plaintiffs sought to introduce at trial. Fed.Rules Evid.Rule 106, 28 U.S.C.A.

[6] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply

170Ak1636 Failure to Comply; Sanctions

170Ak1636.1 k. In General. Most Cited Cases

Once spoliation has been established, the court enjoys considerable discretion over whether to sanction the offending party.

[7] Federal Civil Procedure 170A 2820

170A Federal Civil Procedure
170AXX Sanctions
170AXX(D) Type and Amount
170Ak2820 k. Non-Monetary Sanctions. Most Cited Cases

Dismissal of the entire lawsuit is a sanction traditionally reserved for the most extreme of cases.

[8] Federal Civil Procedure 170A 2173

170A Federal Civil Procedure
170AXV Trial
170AXV(G) Instructions
170Ak2173 k. Necessity and Subject Matter. Most Cited Cases

Pursuant to adverse inference jury instruction, a trier of fact may, but need not, infer from a party's obliteration of a document relevant to a litigated issue that the contents of the document were unfavorable to that party.

[9] Federal Civil Procedure 170A 2173

170A Federal Civil Procedure
170AXV Trial
170AXV(G) Instructions
170Ak2173 k. Necessity and Subject Matter. Most Cited Cases

To qualify for an adverse inference jury instruction, defendants must proffer evidence sufficient to show that the party who destroyed the document knew of: (1) the claim, that is, the litigation or the potential for litigation, and (2) the document's potential relevance to that claim.

Enrique J. Mendoza–Mendez, Mendoza Law Office, San Juan, PR, Juan R. Davila–Diaz, for Plaintiffs.

Marta D. Masferrer, Marta Masferrer Law Office, San Juan, PR, for Defendants.

MEMORANDUM AND ORDER

BESOSA, District Judge.

***1** On September 30, 2013, defendants filed a motion *in limine* requesting that the Court exclude all text messages sent and received between plaintiff Jonathan Polo–Echevarria ("Polo") and prpng@hotmail.com or "Siempre Atento" at trial. (Docket No. 92.) They claim that Polo's own admission that certain text messages were deleted from his phone precludes the use of *any messages* whatsoever, (Docket No. 92), and they submit that the "complaint must be dismissed with prejudice since the case is based on those printed text messages...." (Docket No. 128 at p. 10.)

While their motion *in limine* was pending, defendants received documents in response to an *ex-parte* subpoena to T–Mobile that they had issued-unbeknownst to plaintiffs or the Court—on August 23, 2013. The documents T–Mobile produced in response to the subpoena contain Polo's phone and text messaging records from December 1, 2010 to March 1, 2011. (Docket No. 158–1.) Defendants informed the Court of the phone and text logs in a supplemental motion *in limine*, in which they again request that plaintiffs' case be dismissed due to spoliation of evidence and plaintiffs' bad faith.[FN1] (Docket Nos. 143 and 167.)

--- F.Supp.2d ----, 2014 WL 171599 (D.Puerto Rico)
(Cite as: 2014 WL 171599 (D.Puerto Rico))

I. Plaintiffs' Motion to Quash

[1] As a preliminary matter, plaintiffs argue that defendants' T–Mobile subpoena should be quashed as procedurally defective for failure to give pre-service notice. (Docket No. 144 at p. 2.) Pursuant to Federal Rule of Civil Procedure 45(b)(1), which was in effect at the time defendants issued the subpoena to T–Mobile, a subpoena commanding the production of documents and electronically stored information requires that notice be served on each party before service. The Advisory Committee Notes have defended similar provisions as attempting to "achieve the original purpose of enabling the other parties to object or to serve a subpoena for additional materials...." *See* Fed.R.Civ.P. 45(a)(4).

Defendants issued the subpoena to T–Mobile before the discovery deadline; had plaintiffs objected, the Court would probably not have quashed defendants' subpoena—just as it did not quash plaintiffs' subpoena to attain Rodriguez's AT & T records. (*See* Docket Nos. 59 & 70); (*See also* Docket No. 61) (plaintiffs' admission that "[t]he fact that there were telephone conversations between plaintiff and defendant Rodriguez is certainly relevant and fair game here. It is corroboration of plaintiff's testimony"). Thus, quashing the subpoena now for failing to give timely notice would only result in its re-issuance. Given that trial is less than two weeks away, a re-issuance would promote inefficiency, delay, and undue costs on the litigants. *See, e.g. Richardson v. Axion Logistics, LLC,* 2013 U.S. Dist. LEXIS 144440 (M.D.La. Oct. 7, 2013).

Furthermore, the Court finds defendants' late disclosure of the T–Mobile records to be harmless to plaintiffs. Plaintiffs do not advance any argument demonstrating prejudice resulting from the late production of the records, and the Court finds no basis for concluding either that the defendants are attempting to engage in trial by ambush or that the T–Mobile information otherwise affects plaintiffs' ability to litigate their case. *Cf. Klonoski v. Mahlab,* 156 F.3d 255, 270–71 (1st Cir.1998) (finding defendants' late disclosure of letters significantly prejudiced plaintiff because "it was devastating to his ability to succeed with the jury"). To the contrary, the records merely reveal information personally known to Polo, and the plaintiffs will have had more than one month to review the records before going to trial. (Docket No. 144 at p. 2.) Accordingly, the Court **DENIES** plaintiffs' motion to quash the T–Mobile subpoena.

II. Defendants' Motions *in Limine*

***2** [2] Arguing that Polo engaged in spoliation and that the case therefore must be dismissed, defendants direct the Court to the T–Mobile records. They point out that Polo received numerous messages—the Court counts 22 messages from prpng@hotmail.com between December 31, 2010 and January 7, 2011 and 16 messages from prpng@hotmail.com between February 4, 2011 and February 7, 2011–that were not among the messages plaintiffs produced in discovery. (Docket No. 158–1 at pp. 90–94.) That estimate does not include the numerous text messages that Polo sent in response. (*See* Docket No. 167 at pp. 7–10.)

[3][4] The Court finds that spoliation occurred in this case. A party has a general duty to preserve relevant evidence once it has notice of or reasonably foresees litigation; failure to preserve the evidence constitutes spoliation. *Gomez v. Stop & Shop Supermarket Co.,* 670 F.3d 395, 399 (1st Cir.2012); *see also Perez–Garcia v. P.R. Ports Auth.,* 871 F.Supp.2d 66, 69 (D.P.R.2012) (citing *Zubulake v. UBS Warburg LLC,* 220 F.R.D. 212, 216 (S.D.N.Y.2003)). "The duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation." *Silvestri v. Gen. Motors Corp.,* 271 F.3d 583, 591 (4th Cir.2001). It cannot be disputed that all messages and phone calls between Polo and Rodriguez, and Polo and the prpng@hotmail.com and "Siempre Atento" users, are relevant to plaintiffs' lawsuit.

(Docket Nos. 61 & 145.) Polo admits to forwarding some messages received from prpng@hotmail.com and "Siempre Atento" to himself so that he "would be able to print" them, (Docket No. 98–1 at p. 44), and the record reflects that he did so as early as 12:09:46 p.m. on February 8, 2011. (Docket No. 92 .) The T–Mobile records also reveal that by that time, Polo had contacted his attorney. (Docket No. 158–1 at p. 65.) At a bare minimum, Polo's decision not to forward or save the unproduced texts and photos from prpng@hotmail.com constitutes "conscious abandonment of potentially useful evidence" that indicates that he believed those records would not help his side of the case. *Nation–Wide Check Corp. v. Forest Hills Distribs., Inc.*, 692 F.2d 214, 219 (1st Cir.1982). The record thus indicates that Polo reasonably foresaw litigation and had a duty to preserve relevant evidence, and spoliation occurred.

[5][6][7][8] Once spoliation has been established, the Court enjoys considerable discretion over whether to sanction the offending party. *See Booker v. Mass. Dep't. of Pub. Health*, 612 F.3d 34, 46 (1st Cir.2010). The only sanction defendants identify in their motions *in limine* is dismissal of the entire lawsuit; that sanction is traditionally reserved, however, for the most extreme of cases. *Benitez–Garcia v. Gonzalez–Vega*, 468 F.3d 1, 5 (1st Cir.2006) ("[I]t has long been our rule that a case should not be dismissed with prejudice except when a plaintiff's misconduct is particularly egregious or extreme."). The Court regards an adverse inference instruction [FN2] as the most appropriate sanction in this case. Pursuant to that doctrine, "a trier of fact may (but need not) infer from a party's obliteration of a document relevant to a litigated issue that the contents of the document were unfavorable to that party." *Testa v. Wal–Mart Stores, Inc.*, 144 F.3d 173, 177 (1st Cir.1998).

***3** [9] To qualify for an adverse inference instruction, defendants must "proffer[ ] evidence sufficient to show that the party who destroyed the document knew of (a) the claim (that is, the litigation or the potential for litigation), and (b) the document's potential relevance to that claim." *Booker v. Mass. Dep't of Pub. Health*, 612 F.3d 34, 46 (1st Cir.2010). The Court finds that defendants easily meet their burden. It is reasonable to conclude that the mere act of Polo forwarding himself some messages from prpng @hotmail.com on February 8, 2011—the same day that he submitted a sexual harassment complaint to CPS—reveals his understanding that those messages were relevant to a potential claim against Rodriguez. Even if Polo's behavior does not amount to bad faith, his selective retention of certain messages over the 38 messages that had been received from prpng@hotmail.com and his respective responses, indicates his belief that the records would not help his side of the case. *See Nation–Wide Check Corp.*, 692 F.2d at 219. Thus, Polo knew of both the potential for litigation and the potential relevance of the unproduced messages to that claim. His failure to preserve those messages severely prejudices defendants by precluding a complete review of the conversations and pictures sent between Polo and prpng@hotmail.com. It also prevents defendants from introducing, pursuant to Fed.R.Evid. 106, other writings "that in fairness ought to be considered at the same time" as the messages that plaintiffs seek to introduce at trial. Finally, it impedes defendants from offering evidence pertinent to their defense that prpng@hotmail.com's identity cannot be determined—and is not defendant Rodriguez. Due to those circumstances, and in light of the First Circuit Court of Appeals' indication that "above all else[,] an instruction must make sense in the context of the evidence," *Laurent*, 607 F.3d at 903, the Court will give an adverse inference instruction at trial against plaintiff Polo regarding the more than 38 missing communications between Polo and prpng@hotmail.com.

III. Conclusion

For the reasons discussed above, the Court **DENIES** plaintiffs' motion to quash, (Docket No. 144), and **GRANTS IN PART and DENIES IN PART** defendants' motions *in limine*, (Docket Nos. 92 and

167). An adverse inference instruction regarding the 24 missing communications between Polo and prpng @hotmail.com, and Polo and Rodriguez, will be given at trial.

IT IS SO ORDERED.

FN1. Although defendants received the requested records on October 9, 2013, defendants waited to produce the records to plaintiffs until December 23, 2013, just prior to filing the pretrial report. Defendants' proposed reason for not producing the responsive documents when they received them is that they intended to limit the use of the evidence "for impeachment purposes." (Docket No. 143 at p. 3.) Pursuant to Fed.R.Civ.P. 26(a)(3)(A), a party need not provide the other parties with information about the evidence that it may present at trial if it intends to use the evidence "solely for impeachment." Evidence that is at least in part substantive, meaning that it pertains to the truth of a matter to be determined by the jury, does not fall within the "solely for impeachment" exception of Rule 26(a)(3), and must be produced pursuant to Rule 26. *See Klonoski v. Mahlab,* 156 F.3d 255, 270 (1st Cir.1998) (finding written excerpts of a letter to be substantive evidence "because, separate and apart from whether they contradicted Dr. Klonoski's testimony, they tended to establish the truth of a matter to be determined by the trier of fact," and concluding that the letters should have been produced during discovery) (internal quotations and citation omitted). Because defendants did not timely produce the documents to plaintiffs, defendants would normally be limited to using the same at trial for impeachment purposes only. As discussed in detail below, however, an examination of the T–Mobile records leads the Court to conclude that the effect of plaintiff Polo's spoliation—defendants' inability to invoke Federal Rule of Evidence 106—warrants an adverse inference regarding the missing messages.

FN2. "This permissive negative inference springs from the commonsense notion that a party who destroys a document (or permits it to be destroyed) when facing litigation, knowing the document's relevancy to issues in the case, may well do so out of a sense that the document's contents hurt his position." *Testa,* 144 F.3d at 177.

The First Circuit Court of Appeals has indicated that such an instruction usually is appropriate "only where the evidence permits a finding of bad faith destruction." *United States v. Laurent,* 607 F.3d 895, 902 (1st Cir.2010). It recognizes, however, that "unusual circumstances or even other policies might warrant exceptions." *Id.* at 902–03; *See also Nation–Wide Check Corp. v. Forest Hills Distrib., Inc.,* 692 F.2d 214, 219 (1st Cir.1982).

D.Puerto Rico,2014.
Calderon v. Corporacion Puertorriquena de Salud
--- F.Supp.2d ----, 2014 WL 171599 (D.Puerto Rico)

END OF DOCUMENT

Slip Copy, 2014 WL 4966119 (E.D.N.Y.)
(Cite as: 2014 WL 4966119 (E.D.N.Y.))

United States District Court,
E.D. New York.
Lisa ALTER, Plaintiff,
v.
The ROCKY POINT SCHOOL DISTRICT, and Mr. Michael Ring, Defendants.

No. 13–1100 (JS)(AKT).
Signed Sept. 30, 2014.

Sima Asad Ali, Ali Law Group, P.C., Huntington, NY, for Plaintiff.

Maureen Casey, Ahmuty, Demers & McManus, Esq., Albertson, NY, for Defendants.

MEMORANDUM AND ORDER

A. KATHLEEN TOMLINSON, United States Magistrate Judge.

I. PRELIMINARY STATEMENT

***1** This is a workplace discrimination action brought by Plaintiff Lisa Alter ("Plaintiff") against her former employer Rocky Point School District (the "School District") and Superintendent Michael Ring ("Superintendent Ring"). Beginning in 1987, Plaintiff commenced employment with School District and held a variety of positions throughout her tenure, including second grade teacher, Principal, and Director of Administration. Most recently, prior to her resignation in August 2010, Plaintiff served as Coordinator of Central Registration/Administrative Assistant within the Human Resource Department. While employed in this capacity, Plaintiff alleges that she was subjected to a hostile work environment on the basis of her gender and was retaliated against for complaining to the School District about her treatment, in violation of Title VII of the Civil Rights Act of 1964 ("Title VII") and New York State Human Rights Law ("NYSHRL"). Specifically, Plaintiff claims that during a meeting held on July 2, 2010, Superintendent Ring made multiple gender-based comments in Plaintiff's presence regarding a prospective job applicant. This incident caused Plaintiff discomfort and she lodged a complaint with the School District. However, Plaintiff asserts that the investigation completed by the school district was less than thorough and was overseen by a personal friend of Superintendent Ring. Following her complaint, Plaintiff states that the terms and conditions of her employment fundamentally changed insofar as many of her prior responsibilities were taken away from her. These circumstances caused Plaintiff severe emotional distress and led her to file a complaint about the perceived workplace discrimination in August 2010 with the Rocky Point Board of Education. When she did not hear back from the Board, Plaintiff says she was compelled to submit her resignation, which the Board promptly accepted in August 2010. Plaintiff also asserts claims for disability discrimination and retaliation under the Americans with Disabilities Act ("ADA"), as amended, and the NYSHRL, arguing that Defendants failed to provide her with a reasonable accommodation. Plaintiff brings additional claims under the Family and Medical Leave Act ("FMLA") as a result of Defendants' actions. Specifically, Plaintiff claims that despite notifying Defendants about her serious medical condition, Defendants failed to apprise her of her FMLA rights. Finally, Plaintiff has asserted a claim pursuant to 42 U.S.C. § 1983 against Superintendent Ring for First Amendment retaliation and violation of due process.

Pending before the Court is Plaintiff's second motion to compel discovery and for sanctions.*See* DE 32. Plaintiff argues that Defendants have failed (1) to comply with their obligations to preserve electronic discovery, and (2) to issue a litigation hold to inform

"key players," including Defendant Superintendent Ring, of their obligation to preserve evidence. As a result of these actions, Plaintiff contends that relevant evidence has been subject to spoliation. Plaintiff requests that the Court impose sanctions by means of an adverse inference charge and also award Plaintiff attorneys' fees. Plaintiff further requests that the Court compel Defendants to retain an independent forensic computer expert to oversee all electronic discovery at the School District. Defendants oppose the motion on the grounds that they have complied with their discovery obligations. *See* DE 39. Additionally, Defendants maintain that Plaintiff's arguments regarding spoliation are speculative and unfounded. *Id.* Further, with the Court's permission, Plaintiff filed a motion to supplement the factual record underlying her discovery motion. *See* DE 53. In that supplemental submission, Plaintiff argues that new testimony revealed that several of the Defendants' depositions in February 2014 demonstrates that relevant evidence has been destroyed in this case. *Id.* Second, Plaintiff alleges that Defendants continue to intentionally withhold relevant evidence. *Id.* Defendants also oppose the supplemental motion, contending that their deposition testimony, contrary to Plaintiffs' assertions, does not support such conclusions. *See* DE 56.

***2** For the reasons set forth below, the Court hereby GRANTS, in part, and DENIES, in part, Plaintiff' second motion to compel discovery and for sanctions.

II. BACKGROUND

A. Relevant Procedural History

1. Plaintiff's First Motion to Compel Discovery

Plaintiff filed her first motion to compel discovery on October 1, 2013. *See* DE 17. In that first letter motion, Plaintiff raised objections to the Defendants' responses to her document requests and interrogatories. *Id.* Specifically, Plaintiff sought to compel discovery of Electronically Stored Information ("ESI") in the custody of Defendants, such as e-mails from and between employees of the School District which are relevant to her claims. *Id.*

2. November 4, 2013 Motion Hearing/Status Conference

The parties appeared for a combined motion hearing and status conference on November 4, 2013 at which time the Court addressed Plaintiff's motion. *See* DE 25. The Court issued a number of rulings pertaining to the instant motion at that conference as well. *Id.* For example, the Court advised the parties that "each side has an obligation to supervise its client's discovery efforts" with respect to the "search for ESI." *Id.* ¶ 2. Defendants' counsel advised the Court that she consulted with Assistant Superintendent for Educational Services Susan Wilson regarding the production of ESI in this matter. *Id.* Ms. Wilson was an information technology manager before joining the School District as an Assistant Superintendent. *Id.* Ms. Wilson oversaw ESI searches for the School District. *Id.* The Court, however, expressed concern with the level of consultation between Defendants' counsel and Ms. Wilson:

> While [Defendants' counsel] communicated with Ms. Wilson via telephone and email, she held only one in-person meeting with her client regarding ESI discovery, and she did not directly supervise the discovery. The Court emphasized to [Defendants' counsel] that all counsel in the case are responsible for directly overseeing, supervising and reviewing the discovery efforts taken by the clients. The ultimate responsibility is the attorney's, not the client and there is substantial case law in the Second Circuit confirming counsel's obligations in this regard. Failing to personally oversee searches for relevant discovery leaves an attorney open to sanctions for inadequately supervising such discovery. The clients' representative here, Susan Wilson, conducted the searches, with little direct supervision from [Defendants' counsel] by her own admission.

Id. Thus, in view of this finding, the Court directed Defendants' counsel to "meet immediately with the clients and to review the methodology of the search and the results of the search with her clients to confirm whether all necessary areas have been properly searched and all responsive documents as well as ESI have been produced." *Id.* Further, the Court held that Plaintiff's counsel would be permitted to depose Susan Wilson, if she elected to do so, with the expense to be borne by the Defendants. *Id.*

***3** The Court also directed Defendants to "produce an affidavit from Ms. Wilson within ten days setting forth the particulars of how she conducted the search(es) for relevant documents and ESI responsive to the discovery demands served by the [P]laintiff." *Id.* In particular, the Court directed Ms. Wilson to provide information about "what she turned up in completing those searches." *Id.*

Regarding Plaintiff's request for minutes from the Rocky Point Board of Education meetings, Defendants' counsel reported that the Board meets "publicly and in executive session." *Id.* ¶ 4. According to Defendants' counsel, the Board does not record minutes during these executive sessions. *Id.* The Court thus directed Defendants' counsel to

> provide an affidavit regarding the District's policy or general custom regarding minutes or records of resolutions being taken/reviewed in executive session. The affidavit must also provide information whether there are agendas for the executive sessions and whether those agendas are in writing. If the affidavit does not sufficiently explain the Board's procedures regarding executive sessions, the Court will allow Plaintiff to take depositions of the Board members to obtain the necessary information. The minutes of any public sessions must be produced.

Id. Thus, Plaintiff's October 1, 2013 letter motion to compel was granted, to the extent set forth in the Court's November 4, 2013 Civil Conference Minute Order ("CCMO"). *See generally id.*

B. Plaintiff's Second Motion to Compel Discovery and for Sanctions

Taking the position that Defendants violated the Court's directives, Plaintiff's counsel filed a second motion to compel discovery and for sanctions. *See* Pl.'s Notice of Second Mot. to Compel Disc. and for Sanctions ("Notice of Mot.") [DE 32]. In her supporting memorandum, Plaintiff argues that: (1) sanctions should be imposed against Defendants for their failure to properly institute a litigation hold, complete a good faith search of ESI, and sufficiently oversee ESI searches conducted by Assistant Superintendent Susan Wilson; (2) sanctions should be imposed against Defendants for the spoliation of evidence; (3) an adverse inference charge should be granted against the Defendants in light of their spoliation of relevant evidence; (4) an independent forensic computer expert should conduct electronic discovery of Defendants' systems, computers, emails and devices, with the costs to be borne by Defendants' counsel; and (5) the Court should award Plaintiff's counsel the attorneys' fees and costs associated with bringing this motion. *See* Mem. in Supp. of Pl.'s Second Mot. to Compel Disc. and Mot. for Sanctions ("Pl.'s Mem.") [DE 32–2].

Defendants filed opposition to Plaintiff's motion. *See* Defs.' Mem. in Opp'n to Pl.'s Second Mot. to Compel Disc. and for Sanctions ("Defs.' Opp'n") [DE 39]. They contend that: (1) Plaintiff's arguments rest on a misrepresentation of the factual record; (2) Plaintiff has not demonstrated an entitlement to sanctions under the spoliation doctrine; (3) an adverse inference charge is not warranted given the absence of spoliation; (4) Defendants complied with the Court's November 4, 2013 CCMO and, in any event, no additional ESI search terms were proposed by Plaintiff's counsel at that conference; (5) Plaintiff is not entitled to the appointment of an independent computer forensic expert or attorneys' fees in light of Defendants'

compliance with their discovery obligations. *Id.*

***4** Plaintiff's counsel filed a reply brief in further support of her motion asserting that she has demonstrated sufficient evidence to impose sanctions under Rule 37 on the basis of Defendants' failure to preserve relevant ESI. *See* Pl.'s Mem. in Further Supp. of Pl.'s Second Mot. to Compel Disc. and Mot. for Sanctions ("Pl.'s Reply.") [DE 42]. Plaintiff argues that, on the basis of the record in this case, she is entitled to all the relief requested in her motion (*e.g.* adverse inference charge, appointment of neutral forensic computer expert, and attorneys' fees). *Id.*

C. Plaintiff's Motion to Supplement the Factual Record

With leave of Court, on April 2, 2014, Plaintiff filed a motion to supplement the factual record in support of her second motion to compel and for sanctions. *See* Mot. to Supplement Facts in Supp. of Pl.'s Second Mot. to Compel Disc. and Mot. for Sanctions ("Pl.'s Supp. Mot.") [DE 53]. After taking several depositions of the Defendants on February 26, 27, and 28, 2014, Plaintiff claims to have discovered new testimony relevant to her pending motion to compel. *Id.* at 1. According to Plaintiff's counsel, depositions revealed that: (1) Defendants both failed to preserve and willfully destroyed relevant and material evidence, and (2) Defendants continue to intentionally withhold relevant evidence despite repeated demands for production. *Id.* at 1–6.

Defendants oppose the supplemental motion and dispute the assertions raised by Plaintiff in that motion. *See* Defs.' Mem. in Opp'n to Supplemental Facts in Supp. of Pl.'s Second Mot. to Compel Disc. and for Sanctions ("Defs.' Supp. Opp.") [DE 56]. In particular, Defendants argue that their deposition testimony does not indicate that Defendants failed to preserve or willfully destroyed relevant evidence. *Id.* at 1–4. In addition, Defendants contend that they are not withholding any relevant evidence. *Id.* at 5. With the arguments of counsel delineated, the Court now turns to a review of the law governing relevance of discovery materials and spoliation of such materials.

III. THE APPLICABLE LEGAL STANDARDS

A. General Principles of Relevance

Rule 26 of the Federal Rules of Civil Procedure provides for the discovery of relevant, nonprivileged information which "appears reasonably calculated to lead to the discovery of admissible evidence."FED. R. CIV. P. 26(b). " 'Relevance" under Rule 26 'has been construed broadly to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on any issue that is or may be in the case.' " *Oppenheimer Fund, Inc.*, 437 U.S. 340, 351, 98 S.Ct. 2380, 57 L.Ed.2d 253 (1978); *Maresco v. Evans Chemetics, Div. of W.R. Grace & Co.*, 964 F.2d 106, 114 (2d Cir.1992) (noting that the scope of discovery under Rule 26(b) is "very broad"); *Greene v. City of New York*, No. 08 Civ. 243, 2012 WL 5932676, at *3 (E.D.N.Y. Nov. 27, 2012) (citing *Crosby v. City of New York*, 269 F.R.D. 267, 282 (S.D.N.Y.2010) (explaining that Rule 26 must be construed broadly to include any matter that has, or could reasonably have, bearing on any issue that is, or may be, in the case); *Barrett v. City of New York*, 237 F.R.D. 39, 40 (E.D.N.Y.2006) (noting that the information sought "need not be admissible at trial to be discoverable.").

***5** Notwithstanding the foregoing principles, however, "[t]he party seeking discovery must make a *prima facie* showing that the discovery sought is more than merely a fishing expedition." *Barbara v. MarineMax, Inc.*, No. 12 Civ. 368, 2013 WL 1952308, at *2 (E.D.N.Y. May 10, 2013) (citing *Wells Fargo Bank, N.A. v. Konover*, No. 05 Civ.1924, 2009 WL 585430, at *5 (D.Conn. Mar. 4, 2009); *Evans v. Calise*, No. 92 Civ. 8430, 1994 WL 185696, at *1 (S.D.N.Y. May 12, 1994)). In general, "[a] district court has broad latitude to determine the scope of discovery and to manage the discovery process." *EM*

Ltd. v. Republic of Argentina, 695 F.3d 201, 207 (2d Cir.2012) (citing *In re Agent Orange Prod. Liab. Litig.*, 517 F.3d 76, 103 (2d Cir.2008)); *Barbara*, 2013 WL 1952308, at *3 ("Courts afford broad discretion in magistrates' resolution of discovery disputes."); *Coggins v. Cnty. of Nassau*, No. 07 Civ. 3624, 2014 WL 495646, at *2 (E.D.N.Y. Feb. 6, 2014) (A district court has "broad discretion to determine whether an order should be entered protecting a party from disclosure of information claimed to be privileged or confidential.") (internal quotation omitted).

B. The Doctrine of Spoliation

"Spoliation is the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir.1999); *accord Byrnie v. Town of Cromwell*, 243 F.3d 93, 107 (2d Cir.2001). A court may impose sanctions against a party who spoliates evidence pursuant to Rule 37(b) of the Federal Rules of Civil Procedure as well as through the Court's inherent powers to control the judicial process and the litigation before it. *See Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 106–07 (2d Cir.2002); *West*, 167 F.3d at 779. In situations where sanctions are warranted, district courts have broad discretion in "crafting an appropriate sanction for spoliation." *West*, 167 F.3d at 779; *see Fujitsu Ltd. v. Fed. Express Corp.*, 247 F.3d 423, 436 (2d Cir.2001) ("The determination of an appropriate sanction for spoliation, if any, is confined to the sound discretion of the trial judge...."); *Reilly v. Natwest Mkts. Grp. Inc.*, 181 F.3d 253, 267 (2d Cir.1999) ("Whether exercising its inherent power, or acting pursuant to Rule 37, a district court has wide discretion in sanctioning a party for discovery abuses."). The applicable sanction "should be molded to serve the prophylactic, punitive, and remedial rationales underlying the spoliation doctrine." *West*, 167 F.3d at 779. Stated another way, the selected sanction should be designed to "(1) deter parties from engaging in spoliation; (2) place the risk of an erroneous judgment on the party who wrongfully created the risk; and (3) restore the prejudiced party to the same position he would have been in absent the wrongful destruction of evidence by the opposing party." *Id.* (internal quotation marks omitted); *accord Chin v. Port Auth. of New York & New Jersey*, 685 F.3d 135, 162 (2d Cir.2012).

***6** In some instances, the spoliation of evidence "can support an inference that the evidence would have been unfavorable to the party responsible for its destruction." *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 430 (S.D.N.Y.2004) ("*Zubulake V*") (quoting *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir.1998)). A sanction in the form of an adverse inference instruction is, however, "an extreme sanction and should not be imposed lightly." *Treppel v. Biovail Corp.*, 249 F.R.D. 111, 120 (S.D.N.Y.2008); *see Sekisui American Corp. v. Hart*, 945 F.Supp.2d 494, 497 n. 2 (S.D.N.Y.2003) ("The imposition of sanctions for the spoliation of evidence is a relatively rare occurrence."); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 219 (S.D.N.Y.2003) ("*Zubulake IV*") ("In practice, an adverse inference instruction often ends litigation—it is too difficult a hurdle for the spoliator to overcome.").

A party seeking sanctions has the burden of establishing "(1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a 'culpable state of mind'; and (3) that the destroyed evidence was 'relevant' to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense." *Residential Funding Corp.*, 306 F.3d at 107 (quoting *Byrnie*, 243 F.3d at 107–12); *accord Centrifugal Force, Inc. v. Softnet Commc'n, Inc.*, 783 F.Supp.2d 736, 741 (S.D.N.Y.2011); *Zubulake V*, 229 F.R.D. at 430. With these principles in mind, the Court now addresses the specific circumstances of this case.

IV. DISCUSSION

A. Withholding of Relevant Evidence

The Court is not convinced that, as Plaintiff asserts, Defendants are withholding relevant ESI which is purportedly in their custody. Defendants provided evidence that a system known as "Gaggle" retains all of the School District employee e-mails. Although Plaintiff claims that this system can produce e-mails which include metadata, the e-mails provided to Plaintiff lack such data. Defendants have provided in native format three Word documents, a number of e-mails in. pst format and electronic copies of the Board of Education minutes and agendas for May 2010 to September 2010. *See* Pl.'s Mem. at 6; Def.'s Opp'n at 7. Plaintiff's counsel has provided no factual support from which to draw an inference that the metadata at issue will hold relevant evidence. Because counsel's argument is speculative, it is unavailing.

Plaintiff contends that Defendants' lack of compliance with the Court's November 4, 2013 CCMO is reflected in the lack of discovery exchanged by Defendants since that conference. However, Plaintiffs arguments are not supported by any details or specific reasons why that is the case. In her supplemental motion, Plaintiff states that, despite calling for the production of relevant documents and ESI at the February 2014 depositions, Defendants have not served responses. *See* Pl.'s Supp. Mot at 4–5. On that basis, Plaintiff concludes that Defendants are intentionally withholding relevant evidence. *Id.* Further, as counsel for both sides have repeatedly been instructed in this case, the parties have an obligation to meet and confer regarding these requests before anyone seeks Court intervention, pursuant to Local Civil Rule 37.3. To the extent that Defendants have not responded to the set of discovery requests identified in the Plaintiff's Supplemental Motion, the Court is directing Defendants to answer and to provide substantive information within fourteen (14) days. *See Alexander Interactive, Inc. v. Adorama, Inc.*, No. 12 Civ. 6608, 2014 WL 61472, at *5 n. 2 (S.D.N.Y. Jan.6, 2014) ("While Rule 34 contemplates only written document requests, it is common practice in this District for lawyers to make oral requests during depositions.") (citing *Jackson v. Novell, Inc.*, No. 94 Civ. 3593, 1995 WL 144802, at *1 (S.D.N.Y. April 3, 1995)). Oral requests for documents made during depositions may be enforced in motions to compel. *Id.* (citing same). Lawyers often "follow up oral requests for documents made at a deposition with a confirming letter." *Id.* (quoting *Employers Ins. Co. of Wausau v. Nationwide Mutual Fire Ins. Co.*, No. 05 Civ. 0620, 2006 WL 1120632, at *2 (E.D.N.Y. Apr. 26, 2006)). Plaintiff's right to address those responses with the Court, if necessary, is preserved.

***7** Further, Plaintiff claims Defendants are flouting their discovery obligations because Defendants' counsel identified 113 Word documents and 52 Excel files related to Plaintiff and never produced these documents. *See* Pl.'s Reply at 2; *see also* Defs.' Opp'n at 11. Defendants dispute this characterization and assert that Assistant Superintendent Wilson testified that "113 Word documents and 52 Excel files were recovered from Lisa Alters' [*sic*] computer through the use of recovery software called Active Uneraser." *Id.* According to Defendants, however, "Wilson never identified 113 Word documents and 52 Excel files *related* to Lisa Alter." *Id.* (emphasis supplied). A review of the relevant testimony supports Defendants' interpretation. As to the consultant from Core BTS who was retained by the School District to review Plaintiff's computer, Wilson testified as follows:

> Q. What did you tell him then?
>
> A. I wanted to understand where Lisa had left off since I had to assume her job responsibilities and I wanted to look at the files and correspondence and have access to information. At that time I discovered that there were only three files on the network since 2008. Everything else predated that.

> I had him come over and take a look at the actual machine. *This was unrelated to the cases.* And he had a product called Active Uneraser and it was his own personal product, from what he told me, and he had a license for it and he ran it on the machine, recovered 150—113 Word documents and 52 Excel files. That's an approximation.

See Jan. 15, 2014 Dep. of Susan Wilson annexed to Defs.' Opp'n as Ex. B [DE 39–2] at 16:6–23 (emphasis supplied). Defendants argue that that Plaintiff "fails to understand" that although these documents were identified, none of them were responsive to Plaintiff's discovery demands. *See* Defs.' Opp'n at 11. Plaintiff contends that the mere existence of these documents necessarily indicates that they are relevant to her claims. *See* Pl.'s Reply at 2. In reviewing Wilson's testimony, the Court does not necessarily draw the same conclusion. However, to resolve this issue once and for all, the Court is directing Defendants' counsel to submit the 113 Word documents and 52 Excel files for an *in camera* inspection. These materials are to be delivered to the Court within fourteen (14) days.

In addition, to the extent Plaintiff argues that the Defendants are performing inadequate keyword searches in order to withhold evidence, the Court disagrees. Defendants have produced to Plaintiff three supplemental discovery responses and two CDs which contain ESI materials. Moreover, during her deposition, Susan Wilson testified, in detail, about the number of keyword searches which were conducted to locate relevant ESI materials. These efforts, the Court finds at this time, were sufficient and consistent with the directives in the Court's November 4, 2013 CCMO. If Plaintiff proposes that Defendants are obligated to employ additional search terms in their review of ESI, Plaintiff is directed to confer with Defendants' counsel to arrange for such searches to be made. Again, the Court will not entertain further motion practice concerning this issue until the parties can certify their compliance with Local Civil Rule 37.3.

B. Duty to Preserve

***8** The first element a party must show when seeking sanctions for the destruction of evidence is "that the party having control over the evidence had an obligation to preserve it at the time it was destroyed." *Chin*, 685 F.3d at 162; *Residential Funding Corp.*, 306 F.3d at 107. The Second Circuit has determined that "[t]he obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation." *Fujitsu*, 247 F.3d at 436 (citing *Kronisch*, 150 F.3d at 126). Pursuant to this obligation, "anyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary." *Zubulake IV*, 220 F.R.D. at 217; *accord Curcio v. Roosevelt Union Free Sch. Dist.*, 283 F.R.D. 102, 108 (E.D.N.Y.2012). "In this respect, 'relevance' means relevance for purposes of discovery, which is 'an extremely broad concept.' " *Orbit One Commc'ns, Inc.*, 271 F.R.D. at 436 (quoting *Condit v. Dunne*, 225 F.R.D. 100, 105 (S.D.N.Y.2004)). Therefore, "[w]hile a litigant is under no duty to keep or retain every document in its possession [,] it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request." *Zubulake IV*, 220 F.R.D. at 217 (internal quotations and alterations omitted); *see Scalera v. Electrograph Sys., Inc.*, 262 F.R.D. 162, 171 (E.D.N.Y.2009).

The duty to preserve arises, not when litigation is certain, but rather when it is "reasonably foreseeable." *Byrnie*, 243 F.3d at 107; *see In re Vitamin C Antitrust Litig.*, No. 05 Civ. 453, 2013 WL 504257, at *9 (E.D.N.Y. Feb. 8, 2013) ("[T]he law is clear that the obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation, and that this obligation may arise prior to the filing of

a suit if the litigation is reasonably anticipated.") (quotations omitted); *Toussie v. Cnty. of Suffolk*, No. 01 Civ. 6716, 2007 WL 4565160, at *6 (E.D.N.Y. Dec.21, 2007); *F.D.I.C. v. Malik*, No. 09 Civ. 4805, 2012 WL 1019978, at *1 n. 1 (E.D.N.Y. Mar. 26, 2012) (holding that duty to preserve arose when attorneys who allegedly destroyed documents represented the plaintiff in the underlying transaction at issue); *In re Semrow*, No. 03 Civ. 1142, 2011 WL 1304448, at *3 (D.Conn. Mar. 31, 2011) (holding that duty to preserve vessel arose prior to commencement of suit because the fact that fatalities occurred should have put party on notice of future litigation); *Siani v. State Univ. of New York at Farmingdale*, No. 09 Civ. 407, 2010 WL 3170664, at *6 (E.D.N.Y. Aug. 10, 2010) (holding that receipt of letter informing defendants of alleged discrimination and intent to pursue claim triggered duty to preserve); *Creative Res. Gr. of New Jersey, Inc. v. Creative Res. Grp.*, 212 F.R.D. 94, 106 (E.D.N.Y.2002) (concluding that the duty to **preserve** arose months prior to the commencement of the lawsuit when the problems that eventually led to the filing of the lawsuit first surfaced).

***9** Plaintiff argues that Defendants have breached their duty to **preserve** ESI including, *inter alia*, e-mails, data kept on backup drives, **text messages**, and voicemails. With respect to the ESI that *was* produced, Plaintiff contends that Defendants have failed to provide it in native format, thereby depriving Plaintiff from accessing any associated metadata. According to Plaintiff, the failure of Defendants' counsel to timely and comprehensively advise the key custodians of discovery in this action regarding their preservation obligations has resulted in what Plaintiff claims is spoliation of relevant evidence.

Critically, according to Plaintiff's counsel, Defendants failed to issue a litigation hold until April 2013, more than two years after the Plaintiff filed her Notice of Claim in November 2010. Plaintiff correctly points out that Defendants were obligated to issue litigation holds as soon as the Notice of Claim was filed in November 2010—at which point litigation was or should have been reasonably anticipated by the Defendants. *See Sekisui American Corp.*, 945 F.Supp.2d 494 (finding gross negligence where plaintiff delayed instituting litigation hold until fifteen months after notice of claim and failed to notify IT vendor responsible for preserving ESI for an additional six months). The Court finds it especially troubling that Defendants did not communicate the necessity for a litigation hold to named Defendant Michael Ring until April 29, 2013.

More pointedly, Plaintiff's counsel states that Defendants' counsel "completely failed to discuss a litigation hold with key players." *See* Pl.'s Reply at 2. These "key players" include District Business Manager Greg Hilton, School District Attorney David Pearl, School Board President Michael Nofi, Superintendent Dr. Carla D'Ambrosio, District Clerk Patricia Jones, and Administrative Assistant Loretta Sanchez. *Id.* The Court finds that Defendants had a duty to preserve relevant discovery from these custodians. First, Greg Hilton was specifically mentioned in Plaintiff's Complaint as the other individual present at the meeting held on June 2, 2010. *See* Compl. ¶ 23. Hilton was also in the same room when Superintendent Ring purportedly made the sexist remarks alleged by Plaintiff. *Id.* ¶¶ 23–24. Thus, Mr. Hilton should have been apprised of his duty to preserve relevant evidence as a potential witness in this matter. Similarly, any discovery in the possession of Attorney Pearl would be highly relevant given his role in overseeing the investigation of Plaintiff's allegations against Superintendent Ring. *Id.* ¶ 40. David Pearl was the School District Attorney who issued the report finding that Plaintiff's complaint was not supported by the evidence. *Id.* ¶ 43. Defendants argue that they were under no obligation to preserve any potential discovery by non-parties such as Attorney Pearl. Nonetheless, as an employee or contractor of the School District, Defendants' counsel should have communicated to Attorney Pearl that he may be a custodian of documents and/or information which goes directly to the

claims in this case, especially in light of his role in the events alleged. As an attorney, the Court assumes David Pearl was aware of his preservation obligations in these circumstances.

***10** Further, Defendants failed to discuss a "litigation hold" with School Board President Michael Nofi. Just one day following the June 2, 2010 incident, Plaintiff met with Mr. Nofi to provide him with details of her sexual harassment claim. Compl. ¶ 35. To the extent that any materials and/or relevant notes were created as a result of that meeting, those materials would be relevant to Plaintiff's claims. Plaintiff also had discussions about the sexual harassment incident with Superintendent D'Ambrosio and explained her aversion to hiring School District Pearl to investigate the matter. Defendants had an obligation to ensure that any relevant materials in the possession of these custodians was preserved for the period at issue

Plaintiff also contends that Defendants' failure to stop the overwriting of backup drives constitutes a breach of Defendants' preservation obligations. According to Plaintiff's counsel, these drives could have contained relevant materials regarding Plaintiff's claims. Defendants contend that "[w]hile [they] did not place a hold on the backup drive ... this was because the backup drive is of limited capacity, and cessation of overwriting would cause all subsequently deleted documents to not even reach the back-up drive in the first place." *See* Defs.' Opp'n at 18. Notwithstanding the technical argument asserted by Defendants, at the latest by November 2010, Defendants should have preserved all ESI regarding the Plaintiff from Superintendent Ring and all key custodians in separate backup tapes or in some other medium. Moreover, Defendants assure the Court that all School District e-mails are archived in the Gaggle system. However, ESI does not consist solely of e-mail production.

Finally, Defendants claim that they were not obliged to preserve work-related ESI which employees such as Defendant Superintendent Ring utilized on their personal computers. However, to the extent that the School District employees had documents related to this matter, the information should have been preserved on whatever devices contained the information (*e.g.* laptops, cellphones, and any personal digital devices capable of ESI storage).

C. Culpable State of Mind

"Even where the preservation obligation has been breached, sanctions will only be warranted if the party responsible for the loss had a sufficiently culpable state of mind." *In re WRT Energy Sec. Litig.*, 246 F.R.D. 185, 195 (S.D.N.Y.2007); *see Residential Funding*, 306 F.3d at 107–08. Failures to preserve relevant evidence occur " 'along a continuum of fault-ranging from innocence through the degrees of negligence to intentionality." *Reilly*, 181 F.3d at 267 (quoting *Welsh v. United States*, 844 F.2d 1239, 1246 (6th Cir.1988)). In this Circuit, "the 'culpable state of mind' factor is satisfied by a showing that the evidence was destroyed 'knowingly, even if without intent to breach a duty to preserve it, or negligently." *Residential Funding Corp.*, 306 F.3d at 108 (quoting *Byrnie*, 243 F.3d at 109) (internal alterations and emphasis omitted); *Curcio*, 283 F.R.D. at 111. "In the discovery context, negligence is a failure to conform to the standard of what a party must do to meet its obligation to participate meaningfully and fairly in the discovery phase of a judicial proceeding." *In re Pfizer Secs. Litig.*, 288 F.R.D. 297, 2013 WL 76134, at * 14 (S.D.N.Y.2013).

***11** Although the failure to institute a "litigation hold" is not gross negligence *per se*, whether the party implemented good document or evidence preservation practices is a factor that courts should consider. *Chin*, 685 F.3d at 162; *see Orbit One Commc'ns, Inc. v. Numerex Corp.*, 271 F.R.D. 429, 441 (S.D.N.Y.2010). The Court notes further that "[t]he preservation obligation runs first to counsel, who has a duty to advise his client of the type of information potentially relevant to the lawsuit and of the necessity of preventing

its destruction." *Orbit One Commc'ns*, 271 F.R.D. at 437 (quoting *In re NTL, Inc. Secs. Litig.*, 244 F.R.D. 179, 197–98 (S.D.N.Y.2007)); *Neverson–Young v. BlackRock, Inc.*, No. 09 Civ. 6716, 2011 WL 3585961, at *3 (S.D.N.Y. Aug. 11, 2011) (finding plaintiff who donated her laptop "merely negligent" based on the fact that "[i]n contrast to corporate actors ... [plaintiff] is unsophisticated and unaccustomed to the preservation requirements of litigation.").

The Defendants in this case were negligent with respect to satisfying their obligations to preserve relevant discovery by the key individuals identified in Plaintiff's Complaint, including a named Defendant. *See Cohalan v. Genie Industries, Inc.*, No. 10 Civ. 2415, 2013 WL829150, at *9 (S.DN.Y. Mar. 1, 2013) (finding "evidence in the record that might support a finding of negligence" but not bad faith, where a personnel lift that tipped over and injured the plaintiff was destroyed after two years after the accident during which time numerous photographs, surveillance video, depositions, and inspection of the lift was afforded prior to its destruction). The Court, however, does not conclude that these actions were intentional. In light of Susan Wilson's testimony regarding the School District's ESI storage and review processes, the Court finds that Defendants made an attempt to comply with their discovery obligations once this lawsuit was initiated. However, as pointed out, the fact a litigation hold was not initiated until well over two years after the Notice of Claim was filed is troubling. Defendants' failure to find alternatives for the auto-delete functions of their shared network drive is also problematic. Also of concern to the Court is the earlier acknowledgment by Defendants' counsel that counsel did not directly oversee or engage in the School District's discovery/ESI collection efforts from the beginning. Notwithstanding those facts, the Court does not find an intent to spoliate material evidence here on the basis of the arguments made by Plaintiff's counsel, including the lack of specific (rather than speculative) evidence supporting the spoliation contention.

D. Relevance

Relevance may be assumed where the breaching party acted in bad faith or with gross negligence. *Neverson–Young*, 2011 WL 3585961 at *2; *Orbit One Comm'cns*, 271 F.R.D. at 441 (refusing to presume relevance where the evidence was merely destroyed due to the party's failure to abide by recommended preservation practices). However, where the spoliating party has acted only negligently, the moving party must make a showing that the lost materials were relevant. *In re Pfizer*, 288 F.R.D. 297, 2013 WL 76134, at * 15; *Harkabi*, 275 F.R.D. at 419–20. A party may establish relevance by " 'adducing sufficient evidence from which a reasonable trier of fact could infer that the destroyed or unavailable evidence would have been of the nature alleged by the party affected by its destruction.' " *Harkabi*, 275 F.R.D. at 420 (quoting *Residential Funding Corp.*, 306 F.3d at 109) (internal alterations omitted). "Courts must take care not to hold the prejudiced party to too strict a standard of proof regarding the likely contents of the destroyed or unavailable evidence because doing so would subvert the purposes of the adverse inference, and would allow parties who have destroyed evidence to profit from that destruction." *Residential Funding Corp.*, 306 F.3d at 109 (internal alterations and citations omitted); *accord Slovin v. Target Corp.*, No. 12 Civ. 863, 2013 WL 840865, at *5 (S.D.N.Y. March 7, 2013).

***12** Since the Court has found that Defendants here have lost materials (*e.g.*, a capture of the shared network drive from 2010 and ESI on personal employee devices) due to their negligence, Plaintiff must next demonstrate that the materials were relevant. *See Simoes v. Target Corp.*, No. 11 Civ.2032, 2013 WL 2948083, at *7 (E.D.N.Y. Jun. 14, 2013) (since destruction of evidence was negligent, moving party faced a higher threshold to prove relevance).

Plaintiff has failed to meet this burden. Apart from speculation that Defendants have intentionally destroyed material evidence, the Court does not find

that Plaintiff has set forth, with any degree of specificity, the materials which would have been helpful in prosecuting her claims. Relevance cannot be established solely on the basis of conjecture. Nor can a finding of relevance be grounded solely on the basis that *some* evidence in the custody of key witnesses no longer exists. Plaintiff has the burden of articulating what that evidence is with some degree of factual detail. *See Simoes,* 2013 WL 2948083, at *7 ("Because the present record does not satisfy the relevance element, plaintiff's motion for spoliation sanctions in the form of an adverse inference must fail."). That factual detail is not present here.

The Court finds that an adverse inference is not warranted in these circumstances. However, the actions (or lack of action) of the Defendants require accountability and necessitate a response. Among other things, the Defendants placed the Plaintiff in the position of having to make this motion. The Court found merit to some of the arguments asserted here and although the Court ultimately has not made a finding of spoliation, some form of sanction is appropriate here. Therefore, the Court is imposing a monetary sanction of $1,500, to be borne equally by the School District and the law firm which represented the School District at the time of Plaintiff's November 2010 Notice of Claim filing. *See Wells Fargo Bank, N.A. v. National Gasoline, Inc.*, No. 10 Civ. 1762, 2011 WL 2490808, at *3 (E.D.N.Y. Jun. 22, 2011) (imposing sanctions, pursuant to Rules 37(a)(5), 37(d)(3), and court's inherent powers, in the amount of $10,446.50 to reimburse plaintiff for expenses in bringing motion to compel); *Dee v. Metro. Transp. Auth.*, No. 08 Civ. 3493, 2008 WL 5253090, at *2 (S.D.N.Y. Dec. 12, 2008) (imposing sanction of $1,500, pursuant to Rule 16(f)(1)(c), on plaintiff's counsel for time expended by defendants' counsel on reporting his failures to the Court and causing defendants' counsel to attend a "substantively useless conference"); *Milton Abeles, Inc. v. Creekstone Farms Premium Beef, LLC,* No. 06 Civ. 3893, 2009 WL 2495802, at *1, 5 (denying motion for reconsideration of court's order imposing sanctions in the amount of $250 upon plaintiff's counsel for failing to certify compliance with Local Civil Rule 37.3 in connection with plaintiff's cross-motion to compel). The Court assumes that the law firm of Ahmuty, Demers & McManus, Esqs. was counsel of record for the School District in November 2010. If that is not the case, counsel should advise the Court immediately. The Court further directs that this sanction be paid to Plaintiff within thirty (30) days.

V. CONCLUSION

***13** For the foregoing reasons, Plaintiff's second motion to compel discovery and for sanctions is GRANTED, in part, and DENIED, in part, to the extent set forth in this Memorandum and Order. In addition, the Court DENIES Plaintiff's request for the appointment of an independent forensic computer expert.

The Court further imposes upon the School District and counsel of record for the School District during the time of Plaintiff's November 2010 Notice of Claim a $1,500 sanction, to be borne equally by counsel and the School District. This sanction is to be paid over to the Plaintiff within thirty (30) days.

SO ORDERED.

E.D.N.Y.,2014.
Alter v. Rocky Point School Dist.
Slip Copy, 2014 WL 4966119 (E.D.N.Y.)

END OF DOCUMENT

708 F.Supp.2d 378
(Cite as: 708 F.Supp.2d 378)

United States District Court,
S.D. New York.
PASSLOGIX, INC., Plaintiff,
v.
2FA TECHNOLOGY, LLC, 2FA, Inc., Gregory Salyards, and Shaun Cuttill, Defendants.

No. 08 Civ. 10986(PKL).
April 27, 2010.

Background: Company in business of developing and selling security-related software for managing access to restricted computerized systems brought action against competitor and its principals for breach of licensing agreement in which defendant purportedly agreed to develop identity-authentication software for plaintiff. Plaintiff brought fraud on court allegation against defendants, alleging they created and sent anonymous e-mail in effort to expand discovery, cause plaintiff competitive harm, and garner favorable settlement, and also alleging competitor engaged in spoliation of evidence.

Holdings: The District Court, Leisure, J., held that:
(1) neither company nor its competitor committed fraud on court;
(2) amendment of defendants' counterclaim to add malicious prosecution claim was not appropriate;
(3) principal had duty to preserve 143 written communications between him and one of plaintiff's former employees;
(4) defendants' failure to preserve communications constituted gross negligence;
(5) deleted communications were relevant;
(6) payment of costs was not appropriate sanction for defendants' spoliation of evidence; but
(7) monetary fine of $10,000 was appropriate sanction for spoliation.

So ordered.

West Headnotes

[1] Federal Civil Procedure 170A 2654

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(G) Relief from Judgment
170Ak2651 Grounds and Factors
170Ak2654 k. Fraud; misconduct. Most Cited Cases

A "fraud on the court" occurs where it is established by clear and convincing evidence that a party has sentiently set in motion some unconscionable scheme calculated to interfere with the judicial system's ability impartially to adjudicate a matter by unfairly hampering the presentation of the opposing party's claim or defense.

[2] Federal Civil Procedure 170A 2654

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(G) Relief from Judgment
170Ak2651 Grounds and Factors
170Ak2654 k. Fraud; misconduct. Most Cited Cases

The essence of fraud on the court is when a party lies to the court and his adversary intentionally, repeatedly, and about issues that are central to the truth-finding process.

[3] Federal Civil Procedure 170A 2654

170A Federal Civil Procedure
170AXVII Judgment

170AXVII(G) Relief from Judgment
170Ak2651 Grounds and Factors
170Ak2654 k. Fraud; misconduct. Most Cited Cases

Fraud on the court does not merely embrace any conduct of an adverse party of which the court disapproves; rather, it embraces only that species of fraud which does or attempts to, defile the court itself.

[4] Federal Civil Procedure 170A 2643.1

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(G) Relief from Judgment
170Ak2643 Power of Court
170Ak2643.1 k. In general. Most Cited Cases

The court has inherent authority to conduct an independent investigation in order to determine whether it has been the victim of fraud.

[5] Federal Civil Procedure 170A 2791

170A Federal Civil Procedure
170AXX Sanctions
170AXX(B) Grounds for Imposition
170Ak2791 k. Misrepresentation or omission of facts. Most Cited Cases
(Formerly 170Ak2654)

Federal Civil Procedure 170A 2810

170A Federal Civil Procedure
170AXX Sanctions
170AXX(D) Type and Amount
170Ak2810 k. In general. Most Cited Cases

If it is shown by clear and convincing evidence that a party perpetrated a fraud on the Court, the Court may consider the following five factors in determining an appropriate sanction: (1) whether the misconduct was the product of intentional bad faith; (2) whether and to what extent the misconduct prejudiced the injured party; (3) whether there is a pattern of misbehavior rather than an isolated instance; (4) whether and when the misconduct was corrected; and (5) whether further misconduct is likely to occur in the future.

[6] Federal Civil Procedure 170A 2810

170A Federal Civil Procedure
170AXX Sanctions
170AXX(D) Type and Amount
170Ak2810 k. In general. Most Cited Cases

When faced with a fraud on the court, the available sanctions at a court's disposal range from the issuance of a jury charge on falsehoods under oath, to the imposition of attorney's fees occasioned by the conduct in question, and finally to the entry of judgment against the offending party.

[7] Evidence 157 555.4(1)

157 Evidence
157XII Opinion Evidence
157XII(D) Examination of Experts
157k555 Basis of Opinion
157k555.4 Sources of Data
157k555.4(1) k. In general. Most Cited Cases

An expert testifying on the basis of experience may form his conclusions by applying his extensive experience to the facts of the case.

[8] Evidence 157 555.2

157 Evidence
157XII Opinion Evidence
157XII(D) Examination of Experts

157k555 Basis of Opinion
157k555.2 k. Necessity and sufficiency. Most Cited Cases

Where an expert's qualifications and testimony rest on his experience and not on scientific, mathematical or social science studies or calculations, the expert must apply his experience to the facts using the same intellectual rigor a professional in his field would use in practice.

[9] Evidence 157 555.4(2)

157 Evidence
157XII Opinion Evidence
157XII(D) Examination of Experts
157k555 Basis of Opinion
157k555.4 Sources of Data
157k555.4(2) k. Speculation, guess, or conjecture. Most Cited Cases

Contentions that an expert's assumptions are unfounded go to the weight, not the admissibility, of the testimony.

[10] Federal Civil Procedure 170A 2251

170A Federal Civil Procedure
170AXV Trial
170AXV(K) Trial by Court
170AXV(K)1 In General
170Ak2251 k. In general. Most Cited Cases

Where the court acts as the trier of fact, it uses the discretion given to it to parse and evaluate the evidence for its weight and worth.

[11] Evidence 157 570

157 Evidence
157XII Opinion Evidence
157XII(F) Effect of Opinion Evidence
157k569 Testimony of Experts
157k570 k. In general. Most Cited Cases

Pursuant to its role as factfinder, the court may credit an expert's testimony in whole or in part, regardless of whether another expert is called in rebuttal.

[12] Federal Civil Procedure 170A 2654

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(G) Relief from Judgment
170Ak2651 Grounds and Factors
170Ak2654 k. Fraud; misconduct. Most Cited Cases

In action brought by company in business of developing and selling security-related software for managing access to restricted computerized systems against competitor and its principals for breach of licensing agreement, clear and convincing evidence was not presented that one of competitor's principals committed fraud on court by sending anonymous e-mail to one of plaintiff's clients in effort to cause plaintiff competitive harm; one of plaintiff's former employees confessed to sending e-mail and “spoofing” internet address of principal, former employee's motive for sending e-mail was logical, he matched profile of author, his testimony regarding subsequent log-ins was corroborated by e-mail address computer logs, and kind of “spoofing” at issue was not technologically impossible.

[13] Federal Civil Procedure 170A 2654

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(G) Relief from Judgment
170Ak2651 Grounds and Factors
170Ak2654 k. Fraud; misconduct. Most Cited Cases

In action brought by company in business of devel-

oping and selling security-related software for managing access to restricted computerized systems against competitor and its principals for breach of licensing agreement, clear and convincing evidence was not presented that one of competitor's principals committed fraud on court by sending anonymous e-mail to plaintiff which accused plaintiff of using defendant's intellectual property in violation of contractual and ethical obligations; competitor rebutted nearly all of plaintiff's evidence and presented colorable counter-narrative that one of plaintiff's former employees might have authored e-mail, which was corroborated in part by e-mail correspondence and plaintiff's internal investigation.

[14] Federal Civil Procedure 170A 2654

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(G) Relief from Judgment
170Ak2651 Grounds and Factors
170Ak2654 k. Fraud; misconduct. Most Cited Cases

In action brought by company in business of developing and selling security-related software for managing access to restricted computerized systems against competitor and its principals for breach of licensing agreement, clear and convincing evidence was not presented that plaintiff committed fraud on court by fabricating accusations to interfere with ability of court to adjudicate defendants' counterclaims, absent showing by competitor that plaintiff's allegation of fraud was brought for improper purpose.

[15] Federal Civil Procedure 170A 851

170A Federal Civil Procedure
170AVII Pleadings
170AVII(E) Amendments
170Ak851 k. Form and sufficiency of amendment; futility. Most Cited Cases

Leave to amend need not be granted where the proposed amendment would be futile. Fed.Rules Civ.Proc.Rule 15(a)(2), 28 U.S.C.A.

[16] Malicious Prosecution 249 0.5

249 Malicious Prosecution
249I Nature and Commencement of Prosecution
249k0.5 k. Nature and elements of malicious prosecution in general. Most Cited Cases

To recover on a claim of malicious prosecution under New York law, movant must establish that: (1) defendant either commenced or continued a criminal or civil proceeding against him; (2) the proceeding terminated in his favor; (3) there was no probable cause for the criminal or civil proceeding; and (4) the criminal or civil proceeding was instituted with actual malice.

[17] Federal Civil Procedure 170A 851

170A Federal Civil Procedure
170AVII Pleadings
170AVII(E) Amendments
170Ak851 k. Form and sufficiency of amendment; futility. Most Cited Cases

Amendment of defendants' counterclaim to add malicious prosecution claim, under New York law, was futile and thus, was precluded in action brought by company in business of developing and selling security-related software for managing access to restricted computerized systems against competitor and its principals for breach of licensing agreement, absent any showing of probable cause and malice on part of plaintiff.

[18] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Docu-

ments and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

"Spoliation" refers to the destruction or material alteration of evidence or to the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation.

[19] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

The right to impose sanctions for spoliation of evidence arises from a court's inherent power to control the judicial process and litigation, but the power is limited to that necessary to redress conduct which abuses the judicial process.

[20] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

A party seeking sanctions for spoliation of evidence must establish: (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a culpable state of mind; and (3) that the destroyed evidence was relevant to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense.

[21] Federal Civil Procedure 170A 1551

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)1 In General
170Ak1551 k. In general. Most Cited Cases

A litigant has the duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and is the subject of a pending discovery request.

[22] Federal Civil Procedure 170A 1551

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)1 In General
170Ak1551 k. In general. Most Cited Cases

A party is on notice to preserve relevant documents when litigation is reasonably anticipated, and at least by the time the complaint is served.

[23] Federal Civil Procedure 170A 1551

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)1 In General

170Ak1551 k. In general. Most Cited Cases

After obtaining notice of the litigation, a party must suspend its routine document retention and destruction policy and put in place a litigation hold to ensure the preservation of relevant documents.

[24] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

Once on notice of litigation, a party's failure to issue a written litigation hold constitutes gross negligence because that failure is likely to result in the destruction of relevant information.

[25] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

In the spoliation context, a culpable state of mind includes ordinary negligence.

[26] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

When evidence is destroyed in bad faith, that is, intentionally or willfully, that fact alone is sufficient to demonstrate relevance, for purpose of imposition of sanctions for evidence spoliation; by contrast, when destruction is negligent, grossly negligent, or reckless, relevance must be proven by the party seeking sanctions.

[27] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

No matter what level of culpability is found, the spoliating party should have the opportunity to demonstrate that the innocent party has not been prejudiced by the absence of the missing information.

[28] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

A discarded document is “relevant” in the spoliation

context where a reasonable trier of fact could find that the document either would harm the spoliator's case or support the innocent party's case.

[29] Evidence 157 78

157 Evidence
157II Presumptions
157k74 Evidence Withheld or Falsified
157k78 k. Suppression or spoliation of evidence. Most Cited Cases

In context of spoliation of evidence, to have a sufficiently culpable state of mind warranting a relevance inference, a spoliator must have acted in bad faith-that is, intentionally or willfully.

[30] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

In the absence of bad faith destruction of evidence, the moving party may submit extrinsic evidence tending to demonstrate that the missing evidence would have been favorable to it; moreover, when the spoliating party is merely negligent, the innocent party must prove both relevance and prejudice in order to justify the imposition of a severe sanction.

[31] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

To establish that party engaged in spoliation of evidence by deleting the documents at issue, movant must show by a preponderance of the evidence that, for each category of documents: (1) party had a duty to preserve the documents at the time they were destroyed; (2) party destroyed the documents with a culpable state of mind; and (3) the destroyed documents were relevant to movant's claim or defense.

[32] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

In action brought by company in business of developing and selling security-related software for managing access to restricted computerized systems against competitor and its principals for breach of licensing agreement, company had duty to preserve anonymous e-mail received by one of principals containing attachment of plaintiff's functional specifications, as was required for finding of spoliation of evidence; e-mail was particularly germane to underlying litigation involving claim by competitor that company misappropriated its intellectual property, and it could have led to discovery of admissible evidence regarding company's intellectual property safeguarding practices.

[33] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

The failure to implement a litigation hold in order to preclude spoliation of evidence is, by itself, considered grossly negligent behavior.

[34] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

In action brought by company in business of developing and selling security-related software for managing access to restricted computerized systems against competitor and its principals for breach of licensing agreement, one of principals had duty to preserve at least 143 written communications between him and one of company's former employees concerning software maintenance matters and parties' potential business opportunities, as was required for finding of spoliation of evidence; duty to preserve documents relating to underlying litigation extended to documents concerning, but not limited to, misappropriation of intellectual property and the parties' obligations and performance under their licensing agreement, and principal was on notice that some of his written communications with former employee were probative of underlying litigation when communications were deleted.

[35] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

In action brought by company in business of developing and selling security-related software for managing access to restricted computerized systems against competitor and its principals for breach of licensing agreement, failure of one of principals to preserve at least 143 written communications between himself and one of company's former employees concerning software maintenance matters and parties' potential business opportunities constituted gross negligence, as was required for finding of spoliation of evidence; even if former employee was not actively involved in fraud on court dispute, at least two of principal's written communications with employee related to issues involved in underlying litigation.

[36] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

In action brought by company in business of developing and selling security-related software for managing access to restricted computerized systems against competitor and its principals for breach of licensing agreement, 143 deleted written communications between one of principals and one of company's former employees concerning software maintenance matters and parties' potential busi-

ness opportunities were relevant, as was required for finding of spoliation of evidence; some of communications could have cast doubt on competitor's misappropriation claim where competitor, a purported victim of company's misappropriation of its intellectual property, pursued business opportunity with company involving competitor's intellectual property in midst of lawsuit relating to fall-out of prior relationship.

[37] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

The court has the inherent power to impose sanctions for the spoliation of evidence, even where there has been no explicit order requiring the production of the missing evidence.

[38] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

The determination of an appropriate sanction for spoliation, if any, is confined to the sound discretion of the trial judge and is assessed on a case-by-case basis.

[39] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

Sanctions for the spoliation of evidence are meant to: (1) deter parties from destroying evidence; (2) place the risk of an erroneous evaluation of the content of the destroyed evidence on the party responsible for its destruction; and (3) restore the party harmed by the loss of evidence helpful to its case to where the party would have been in the absence of spoliation.

[40] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

A court should always impose the least harsh sanction that can provide an adequate remedy for spoliation of evidence; the choices of sanctions include, from least harsh to most harsh, further discovery, cost-shifting, fines, special jury instructions, preclusion, and the entry of default judgment or dismissal terminating sanctions.

[41] Evidence 157 78

157 Evidence
157II Presumptions
157k74 Evidence Withheld or Falsified
157k78 k. Suppression or spoliation of evidence. Most Cited Cases

An adverse inference is warranted where a party intentionally destroys documents that it is obligated to preserve and that are relevant to its adversary's case.

[42] Federal Civil Procedure 170A 1278

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(A) In General
170Ak1278 k. Failure to respond; sanctions. Most Cited Cases

Evidence reclusion is a harsh sanction preserved for exceptional cases where a party's failure to provide the requested discovery results in prejudice to the requesting party.

[43] Federal Civil Procedure 170A 1637

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1637 k. Payment of expenses. Most Cited Cases

Payment of costs was not appropriate sanction for spoliation of evidence by competitor in action brought by company in business of developing and selling security-related software for managing access to restricted computerized systems against competitor and its principals for breach of licensing agreement; the extra expense incurred by company, related solely to deletion of electronic data and certain information between one of principals and former employee, could not be easily carved out from company's overall costs in litigating dispute.

[44] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

The applicable sanction for spoliation of evidence should be molded to serve the prophylactic, punitive, and remedial rationales underlying the spoliation doctrine.

[45] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

Imposing a fine is consistent with the court's inherent power to sanction parties for the spoliation of evidence.

[46] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

Monetary fine of $10,000 against competitor and its principals was appropriate sanction for their spoliation of evidence in action brought against them by company in

708 F.Supp.2d 378
(Cite as: 708 F.Supp.2d 378)

business of developing and selling security-related software for managing access to restricted computerized systems for breach of licensing agreement; competitor was small company, fine would serve dual purposes of deterrence and punishment, and fine would affect principals directly.

***383** Proskauer Rose LLP, Steven M. Kayman, Esq., Dan Goldberger, Esq., Cadwalader, Wickersham & Taft LLP, Hal S. Shaftel, Esq., New York, N.Y., for Plaintiff.

Laurence Singer, Attorney–at–Law, Laurence Singer, Esq., Washington, D.C., for Defendants.

OPINION AND ORDER

LEISURE, District Judge:

Table of Contents

CONCLUSION

***384** Plaintiff, Passlogix, Inc. (“Passlogix”), brings this fraud on the court allegation against defendants Gregory Salyards, 2FA Technology, LLC, and 2FA, Inc. for creating and sending an anonymous e-mail in an effort to expand discovery, cause Passlogix competitive harm, and garner a favorable settlement. As a remedial measure, Passlogix asks the Court to dismiss 2FA's pleadings and award Passlogix costs and attorneys' fee. Passlogix also alleges that ***385** 2FA engaged in spoliation of evidence and asks for an adverse inference, preclusion, and costs. 2FA counter-alleges that Passlogix committed its own fraud on the court by bringing its erroneous fraud on the court allegation to delay adjudication on the merits.

The Court held a five-day evidentiary hearing on the issues of fraud on the court and spoliation of evidence and asked the parties to submit post-hearing memoranda. For the reasons set forth below, the Court holds that neither Passlogix nor 2FA has established by clear and convincing evidence that a fraud on the court was committed. The Court also holds that 2FA's failure to preserve certain documents led to the destruction of evidence in this case, requiring imposition of a $10,000 monetary fine.

BACKGROUND

Both Passlogix and 2FA Technology, LLC and 2FA, Inc. (collectively, “2FA”) are in the business of developing and selling security-related software for managing access to restricted computerized systems. (Pl. Passlogix's Post–Hearing Mem. (“Mem.”) 1.) The instant dispute arises out of Passlogix's lawsuit against 2FA, and 2FA's principals, Gregory Salyards (“Salyards”) and Shaun Cuttill (“Cuttill”), for breach of a licensing agreement in which 2FA purportedly agreed to develop identity-authentication software for Passlogix. Passlogix seeks (1) money damages against 2FA for breach of contract and tortious interference with business relations, and (2) a declaration that (a) it did not breach the licensing agreement or any other duties owed to 2FA or its employees, including Salyards and Cuttill, (b) 2FA has no valid grounds to terminate the licensing agreement and is obligated to continue abiding by the agreement, (c) Passlogix has not impermissibly used any confidential information or intellectual property of 2FA, and (d) Passlogix does not owe 2FA any money. (Am. Compl. ¶¶ 20–32.) In its Answer, 2FA asserts counterclaims against Passlogix for breach of contract, breach of the covenant of good faith and fair dealing, unfair competition, misappropriation of 2FA's intellectual property, and tortious interference with business relations. (Answer & Countercl. ¶¶ 32–46.)

In addition to the fraud on the court and spoliation allegations addressed in this decision, also pending before the Court is 2FA's motion to reverse Magistrate Judge Dolinger's denial of its motion to compel discovery and 2FA's motion for a preliminary injunction against Passlogix. These motions will be addressed in subsequent decisions.

I. Anonymous E-mails

The instant dispute was triggered by an anonymous e-mail sent on September 3, 2009, 4:00 p.m. Central Daylight Time (“CDT”) from “passlogix- vgo- saw@ hushmail. me” (the “September 3 e-mail”). The September 3 e-mail was sent to Passlogix's President and CEO, Marc Boroditsky, Passlogix's Chief Technology Officer, Marc Manza, two executives at a non-party business entity, Imprivata, Inc. (“Imprivata”), and Salyards and Cuttill.[FN1]

(Passlogix Exhibit ("PX") 1.) The anonymous author, who purports to have "more than 15 years of development experience" and to have transitioned to Passlogix "earlier this year," asserts that Passlogix issued a "recent mandate to utilise Imprivat[a] and 2FA information that clearly oversteps ... contractual and ethical obligations." (*Id.*) The anonymous author claims to be "appalled ***386** by the unprofessionalism and unethical behavior undertaken by the Passlogix engineering management organisation" and to "have been treated like a second-class citizen." (*Id.*) The September 3 e-mail also includes two attachments that contain specifications to Passlogix software under development. (*See id.*); (Evidentiary Hr'g Tr. ("Tr.") 44:23–45:5.) One attachment is titled "Master Func Spec v-GO SAW v1.5" and the other is titled "SAW Func Spec Iteration 2 vl.5." (PX 1; Tr. 45:3–5.)

> FN1. Cuttill never actually received the September 3 e-mail because his e-mail address was misspelled. (Evidentiary Hr'g Tr. ("Tr.") 532:3–11.)

Passlogix claims that the September 3 e-mail was not the first time that it received an anonymous e-mail from a hushmail.com e-mail address, and that on April 13, 2009, 3:59 p.m. CDT, Boroditsky and Mark Gillespie, a Passlogix employee, received an e-mail from "concerned atpass logix@ hushmail. com" (the "April 13 e-mail"). (PX 2.) The April 13 e-mail expresses concern about Passlogix losing "the Wal–Mart deal" and discloses Salyards' close relationship with "Adnan," a principal consultant at Deloitte & Touche who was brokering a deal with Wal–Mart for 2FA. (PX 2; Tr. 417:12–419:6, 542:15–20.) Cuttill testified that this e-mail was "detrimental to 2FA" because it "expose [d] a key relationship that [2FA][was] pursuing to win the Wal–Mart deal," which "was the only way" for a small company like 2FA to get "in front of Wal–Mart," and "exposing that [relationship], in essence, killed [2FA's] opportunity at WalMart." (Tr. 542:3–14.) In fact, Cuttill testified that after April 13, Adnan would not return Cuttill's e-mails. (Tr. 542:15–20.)

By letter dated September 14, 2009, counsel to 2FA wrote to Magistrate Judge Dolinger about the anonymous September 3 e-mail "because of the seriousness of the allegations set forth in the email, especially in light of 2FA's present Motion for Preliminary Injunction, filed on the basis of Passlogix's misappropriation of 2FA's intellectual property." (PX 30 at 2.) In a separate letter dated October 27, 2009, Passlogix alleged that Salyards committed a fraud on the Court by authoring and transmitting the September 3 and April 13 e-mails. (PX 33.) Passlogix alleges that Salyards created and sent these e-mails to expand discovery, cause Passlogix competitive harm, and garner a favorable settlement—all of which constitute a fraud on this Court. (Mem. 6.)

II. Investigation Into Authorship of Anonymous E-mails

Within days of receiving the September 3 e-mail, Passlogix retained outside counsel to conduct an internal investigation into the sender of that e-mail and any evidence supporting the allegations set forth in that e-mail. (Tr. 24:25–25:12, 35:10–36:3; PX 34.) A report following the internal investigation concluded that the claims in the September 3 e-mail were false and that no individual at Passlogix identified any inappropriate request to utilize intellectual property from third parties. (PX 34 & 35; Tr. 36:17–22.)

In addition to its internal inquiry, Passlogix subpoenaed Hushmail.com ("Hush"), the Canadian e-mail service provider through which the September 3 and April 13 e-mails were sent. (Tr. 38:5–21.) Hush provided Passlogix with the Internet Protocol ("IP") address logs for the Hush accounts from which the anonymous e-mails were sent ("Hush logs"). (PX 48 & 49.) "An IP address is a set of numbers ... assigned to a computer in order for it to communicate on a network, which also includes communicating to the outside world; internet, web pages, e-mail as an example." (Tr. 146:20–23.) "An IP log is a log that many companies use to capture the source IP address of the network or computer that's connecting to the ser ***387** vice...." (Tr. 154:3–5.) The Hush logs reveal that both the September 3 and April 13 e-mails were sent from the IP address 70.114.246.62. (PX 48 & 49.) After the April 13

e-mail was sent, Hush captured additional log-ins from the IP addresses 70.114.246.202 and 64.186.161.2. (PX 49.) According to records that Passlogix obtained from Time Warner, the IP address 70.114.246.62 is registered to Salyards at 2FA's office location while the IP address 70.114.204.202 is registered to Salyards' wife, at their home address. (PX 40; Tr. 41:1–23, 156:9–20.) The final IP address—64.186.161.2—appears related to the Mark Hopkins Hotel in San Francisco, where Salyards and Cuttill were staying for a work conference from April 19–April 24, 2009. (PX 37, 38, 49; Tr. 42:14–43:21.)

In addition to the Hush logs, Passlogix points to circumstantial evidence that Salyards authored both anonymous emails. Passlogix contends that the timing of each of the anonymous e-mails is suspect because the April 13 e-mail was sent during the course of a dispute regarding third party discovery subpoenas and the September 3 e-mail was sent one day after Passlogix filed its brief in opposition to 2FA's motion for a preliminary injunction. (Def.'s Ex. ("DX") 1 (Passlogix Ltr. 11/6/09 at 1–2).) Additionally, Passlogix contends that because the September 3 e-mail was sent less than two weeks prior to the parties' settlement conference before Judge Dolinger, Salyards sent the e-mail to procure a more favorable settlement from Passlogix. (Mem. 6.) Salyards admits that he referenced the September 3 e-mail in settlement conversations with Boroditsky in the days following the September 3 e-mail. (*See* PX 29 ("We have a proposal for you that we feel best serves all concerned" (September 5, 2009); "Our attorney plans on raising the [September 3 e-mail] with the court this week, ... I'm in NYC this weekend and would be willing to meet in the event you have a change of heart concerning our recent proposal" (September 12, 2009)); Tr. 338:20–339:13.) Passlogix further asserts that Salyards has admitted to receiving the confidential information attached to the September 3 e-mail from another anonymous e-mail purportedly sent to him from a Hush e-mail address in late June or early July 2009. (PX 33 at 4 n. 1.) Also, Passlogix claims that Salyards may have received the attachments to the September 3 e-mail from a source within Passlogix. (DX 1 (Passlogix Ltr. 11/6/09 at 3).)

Cuttill testified about his own investigation into the origin of the anonymous e-mails. During the second or third week of September 2009, Cuttill and Salyards visited Hush "to find out what Hushmail was all about." (Tr. 576:22–577:16.) In late October or early November 2009—after Passlogix wrote this Court alleging that Salyards was the author of both anonymous emails—Cuttill interviewed 2FA employees that he thought would have had access to 2FA's computer network in April and September and checked all of 2FA's computers for evidence of the attachments to the September 3 e-mail, but found no evidence that anyone at 2FA sent the e-mails. (Tr. 572:16–575:5.) Cuttill did not take notes during his investigation, nor did he memorialize his findings in writing. (Tr. 573:15–16.)

III. Salyards' Defense and "IP Spoofing" Theory

Salyards testified under oath at his October 23, 2009 deposition and during the evidentiary hearing in January 2010 that he was not involved in the transmission of either e-mail. (Tr. 384:25–385:4.) He refutes Passlogix's claim that the confidential attachments to the September 3 e-mail were available to him or to 2FA. (DX 1 (2FA Ltr. 10/29/09 at 3–4 & 2FA Ltr. ***388** 11/9/09 at 3).) He also maintains that the mere content of the April 13 e-mail, which discloses a business opportunity with Wal–Mart that 2FA was pursuing as a competitor to Passlogix, eliminates any motive that Salyards would have in sending that e-mail. (DX 1 (2FA Ltr. 10/29/09 at 2–3).) In arguing that no one at 2FA sent the September 3 e-mail, Salyards points to the use of the letter "s" in the spelling of words such as "organisation" and "utilise" in the e-mail, indicating British or Canadian authorship. (DX 1 (2FA Ltr. 11/9/09) at 3.)

Salyards notes that the IP address linked to the September 3 e-mail is not assigned to him specifically, but rather to 2FA's office location and is used by every computer sending e-mails from that location. (DX 1 (2FA Ltr. 10/29/09 at 2).) Moreover, Salyards contends that he was out with his family and friends at the time the September 3 e-mail was sent at 4:00 p.m. CDT, [FN2] and submitted affidavits from three individuals, two of whom specifically state that Salyards was with them from approximately 3:15

p.m. until 4:30 or 4:45 p.m. on September 3. (*Id.* at 4 & Ex. 2.) 2FA also notes that the anonymous e-mails are not evidence and, notwithstanding the fact that 2FA could have used the allegations in the September 3 e-mail in its reply brief in support of its motion for a preliminary injunction, it did not do so. (DX 1 (2FA Ltr. 11/9/09 at 2).)

> FN2. There is no dispute that Cuttill was vacationing in Mexico when the September 3 e-mail was sent. (DX 1 (2FA Ltr. 10/29/09 at 4).)

Salyards proffers the affirmative defense of IP spoofing, stating that a Passlogix employee may have "spoofed" his IP address in an effort to impersonate him on the internet. (DX 1 (2FA Ltr. 10/29/09 at 1–2).) IP address spoofing is a practice whereby a person can make his true IP address appear to be any address he chooses. (*Id.* at 1.) 2FA asserts that IP spoofing can be accomplished from anywhere, as long as the impersonator knows a user's IP address. (*Id.* at 1; *see also* Tr. 391:22–25 (Salyards defining IP spoofing as "concealing your ... IP address ... and perpetrating to be something else when you're out on the Internet").) Salyards claims that, based on a decade of specialized training in computer security, including hacking and spoofing IP addresses to conduct "penetration testing" of security solutions, he knows how to conceal his IP address and that had he endeavored to create a fictitious e-mail, he would have ensured that it could not be traced back to him personally or to 2FA. (Tr. 389:3–11, 390:13–393:21; DX 1 (2FA Ltr. 10/29/09 at 2).)

IV. Chris Collier's Confession to Sending the April 13 E-mail and "Spoofing" Salyards' IP Address

Chris Collier, a former Passlogix employee who has over ten years of experience in the computer security industry, confessed under oath during a December 2, 2009 deposition that he wrote and sent the April 13 e-mail. (Collier Dep. 5:18–6:23, 8:11–14, 61:3–62:5.) Collier testified that he sent the April 13 e-mail from his personal laptop computer while he was at 2FA's office without the knowledge of 2FA. (Collier Dep. 60:11–62:11, 76:15–19, 83:11–14.) Because he sent the April 13 e-mail from a wireless access point in 2FA's conference room, Collier did not need to spoof 2FA's IP address to make it appear that the e-mail was sent from 2FA. (*Id.* 62:4–8, 84:6–8.) After the initial e-mail was sent from 2FA's office, Collier said that he spoofed 2FA's IP address "[s]ix, maybe seven times" to check whether he received any responses to the April 13 e-mail from the e-mail recipients—Boroditsky***389** or Gillespie. (*Id.* 86:2–4.) During his subsequent log-ins to Hush, Collier said that he concealed his IP address by substituting his IP address with "an IP address from the e-mail headers from Greg [Salyards]," by using software downloaded from the internet. (*Id.* 64:22–25, 70:12–21, 86:11–25.) When asked what program he used to spoof Salyards' IP address, Collier responded, "I can't be sure. Probably Mac IP Change, which is one that I've used many times before. That's the one I used." (*Id.* 86:23–25.) Collier also testified that the source of the content of the April 13 e-mail came from Cuttill, who disclosed to Collier 2FA's efforts to land the Wal–Mart deal during Collier's April 13 visit to 2FA's office. (*Id.* 108:15–110:15.) Collier no longer has the laptop that he used to send the April 13 e-mail because he "decommissioned" it and gave it to a friend in need. (*Id.* 108:11–14; PX 45 at CC–000A ¶ 1.)

Cuttill corroborates Collier's account of visiting 2FA's office on April 13. Cuttill recalls being in the office on April 13 because he was preparing for a work conference ("RSA conference") in California the following week. (Tr. 532:14–533:8.) Cuttill states that Salyards was not in the office because he was watching his children that week since his wife was going to watch them the following week while Salyards was at the RSA conference. (Tr. 533:9–19.) Cuttill states that Collier arrived at 2FA's offices on April 13 "somewhere around 3:00, give or take maybe 15 minutes" to do work on "Oberthur cards." (Tr. 594:9–595:1; 585:13–19.) After Collier arrived, he and Cuttill "chatted for a little bit," "definitely less than ten minutes, probably less than five minutes," about the Wal–Mart deal. (Tr. 585:20–586:1.594:12–25.) Then Cuttill set up Collier with internet in a conference room while Cuttill went to prepare for a 4 p.m. call. (Tr. 585:14–19; 595:1–11.) After Cuttill's 4 p.m. call was over, he and Collier worked on the Oberthur cards until 6 or 6:30 p.m. (Tr. 595:9–23.)

Collier testified that he did not send the September 3 e-mail. (Collier Dep. 65:8–17.) He did state, however, that in June 2009, he had a conversation with another Passlogix employee, Joseph Robinson, who expressed concerns similar to those stated in the September 3 e-mail. (*Id.* 65:18–67:4, 77:17–78:24, 79:7–18.) Collier states that he suggested to Robinson to raise the issue with Boroditsky or, alternatively, send an e-mail through Hush since "[t]hey won't know who you are." (*Id.* 68:7–16, 98:19–99:21.) Collier says that he told Robinson that he used Salyards' IP address when he sent his own anonymous email, though he did not tell Robinson what that IP address was. (*Id.* 98:14–18.) Salyards asserts that Robinson fits the profile of the author of the September 3 e-mail because Robinson lives in Canada, transitioned to Passlogix in April 2009 from a firm bought by Imprivata, the company mentioned in and copied on the September 3 e-mail, had fifteen years of technology experience, and was terminated by Passlogix in October 2009 for unexcused absences. (DX 19; Tr. 80:7–81:5; PX 53 at 2.)

Passlogix states that Collier's confession to sending the April 13 e-mail is unreliable since Collier admitted to lying about his role in the creation of the e-mail when Passlogix interviewed him as part of its internal investigation. (DX 4 at 2.) Passlogix underscores the secretive business ties Collier had with Salyards and Cuttill, evidenced by the fact that Collier testified that Cuttill provided him with the information used to write the April 13 e-mail. (*Id.;* Collier Dep. 53:21–54:2, 114:13–115:8, 118:13–19.) Passlogix also points to inaccuracies in Collier's testimony regarding when and where he created the April 13 e-***390** mail account, his Hush account password, and the extent of his communications with Salyards. (DX 4 at 2.) Collier testified that he set up the Hush account "a few days before the e-mail was sent." (Collier Dep. 84:10–12; 85:20–86:1.) However, the Hush logs indicate that the account was set up on April 13, 2009—the same day the e-mail was sent, just twenty-seven minutes before it was transmitted. (PX 49; PX 44 ¶ 6.) Collier also provided a password that he used for the Hush account, which Hush confirmed was inaccurate. (Collier Dep. 84:17–85:19; PX 41 & 44 ¶ 5.) Collier, however, noted that he could not "remember if that's exactly the password [he] used, because [he had not] been [on the website] for months now." (Collier Dep. 85:18–19.) Additionally, Collier testified that between April 13 and December 2, 2009, he spoke to Salyards "[p]robably 15 to 20 times," while phone records from October 2009 alone show that they spoke over thirty times. (*Id.* 118:13–15; PX 45.) With respect to the September 3 e-mail, Passlogix states that Collier's "suspicions" that Robinson sent that email are inadmissible and unreliable. (Mem. 11.)

V. Expert Testimony Regarding IP Spoofing

The Court qualified Passlogix's expert in computer forensics and computer crime investigations, Andrew Obuchowski, Jr., during a preliminary hearing on November 9, 2009,[FN3] based on Obuchowski's twelve years of law enforcement experience in computer crime forensics and three years of experience in private computer forensics, including "tracing of e-mails" and "analysis of how a computer was used ... during the commission of an incident or crime." (Prelim. Hr'g Tr. 33:6–34:20, 36:11–37:7.) Obuchowski has taught computer crime investigations to law enforcement officers and is an adjunct professor at a criminal justice college in Massachusetts. (*Id.* 33:23–34:5.) Obuchowski has testified in several court proceedings "regarding computer crime and computer forensics," including IP spoofing. (*Id.* 34:6–35:10.)

> FN3. At the end of the preliminary hearing, the Court permitted the parties to conduct additional discovery and reconvene for a more fulsome hearing where all relevant witnesses, particularly Salyards, could be present. (Prelim. Hr'g Tr. 61:22–67:9.)

Obuchowski concludes that spoofing a public IP address assigned by an Internet Service Provider,[FN4] such as Time Warner, "is not possible to the extent of being undetected" because "[t]he email message headers would show inconsistencies ... [that] were not present in the email headers" from the April 13 and September 3 e-mails. (PX 36 ¶ 15; *see also* Tr. 153:9–13, 170:15–18.) Obuchowski

also concludes that the MAC IP Change program that Collier claimed he used to spoof Salyards' IP address "does not have the technical capability of changing an IP address that's assigned by Time Warner to make it appear that you are coming from 2FA's network unless you were actually on 2FA's network." (Tr. 164:6–19.) Obuchowski explains that the MAC IP Change Program only "changes [the] IP address of the computer that you install the software program on," and is not capable of "spoofing an Internet service provider." (Tr. 242:5–11.) Additionally, Obuchowski concludes that he is not "aware of" any "software on the market that can be used to spoof an Internet service provider" and that "any software program install[ed] on a local laptop computer ... would not change the IP ***391** address assigned by an Internet service provider, in the example of Time Warner, that would reflect any change in the Hushmail logs." (Tr. 242:12–16, 623:17–624:2.) Obuchowski explains that, to access a website on the internet, two computers or networks must be able to communicate with each other. (Tr. 146:20–23.) They do so by sending information back and forth to each other's IP address (the same way a telephone number corresponds to a telephone, an IP address corresponds to a computer and/or network). (Tr. 146:20–147:3.) Thus, if someone tried to access Hush and conceal his own IP address by spoofing another IP address, Hush would respond by sending information to the computer/network associated with the "spoofed" IP address, not to the concealed IP address. (Mem. 10.) As a result, the spoofer would never be able to complete the process of logging into the Hush website or complete any other activity on the Hush website because he would not receive communication back from Hush, as it would instead be directed to the spoofed IP address. (*Id.; see also* Tr. 615:8–16.) Obuchowski acknowledges that if Collier sent the April 13 e-mail from 2FA's network, as Collier claims, "then 2FA's IP address would appear in the logs." (Tr. 231:22–25.) However, Obuchowski states that Collier did not send the April 13 e-mail because Collier was incorrect about when the April 13 Hush account was created and about the password he used to create it. (Tr. 165:4–166:25, 168:14–20; PX 41.)

FN4. A private IP address is assigned to a user locally. When a user connects to the internet, the internet service provider (ISP)-Time Warner, in this case-assigns a public IP address. (Tr. 180:24–181:14.)

Obuchowski created his own Hushmail test account during the course of his investigation, even though he did not mention the test account in either one of his declarations. (Tr. 234:10–24; PX 36 & 40.) Obuchowski "walk[ed] through the same steps in creating an e-mail account as Mr. Collier claimed that he did" and sent a test e-mail to his work e-mail address. (Tr. 235:1–6.) Obuchowski only used the test account once to see what services Hush offers and what the e-mail headers look like when a Hush e-mail is received. (Tr. 235:12–19.) Obuchowski stated that the test e-mail he sent appeared just like the other e-mails sent from the April 13 and September 3 e-mail addresses, although he did not have a copy of, or a log from, the test e-mail. (Tr. 235:5–23.) When asked for his password to the Hush account at the evidentiary hearing on January 14, 2010, Obuchowski could not recall; nor could he recall the date that he created the account, but noted that it would have been before his first declaration, which was dated November 6, 2009. (Tr. 235:24–236:5.)

2FA does not proffer a computer forensics expert in rebuttal; instead, it relies on Salyards' and Cuttill's personal experiences to challenge Obuchowski's conclusion about the unfeasibility of IP spoofing. Salyards testified that he has twelve years of experience in computer forensics and computer security, including hacking and spoofing, and has spoofed IP addresses to conduct "penetration testing" of security solutions as part of his work and that he knows how to conceal his IP address. (Tr. 388:19–389:11, 390:13–392:18.) Cuttill, 2FA's Chief Technology Officer, has fourteen years of experience in strong authentication computer software. (Tr. 519:19–521:9.) Cuttill testified that he has spoofed IP addresses by concealing his own IP address and selecting an IP address that belonged to a company's internal network. (Tr. 565:9–567:17.) Cuttill also said that, contrary to Obuchowski's conclusions, he has spoofed a public IP address that has been assigned by an Internet Service Provider, such as Time Warner, as part

of security analysis projects. (Tr. 589:25–591:20.) He said he typically spoofs "by hand" but has used software that helps with encryption matters.***392** (Tr. 591:5–9.) Although he has never used the MAC IP Change program to spoof an IP address, Cuttill noted that there are "a number of programs that are called very similar to that." (Tr. 591:21–592:11.)

Cuttill and Salyards also contend that the Hush logs exonerate Salyards because the Mark Hopkins Hotel, where they stayed from April 19 to April 24, 2009, never assigned Salyards an IP address ending in ".2"—the IP address that the Hush logs captured. (Def.'s Opp'n to Pl. Passlogix's Post–Hearing Mem. ("Opp'n Mem.") 18.) The Hush logs captured two log-ins to Hush from the IP address 64.186.161. *2*—the first on April 20 at 10:30 a.m. Pacific Daylight Time ("PDT") and the second on April 23 at 10:15 p.m. PDT. (PX 49 (emphasis added).) The Mark Hopkins Hotel records indicate that Salyards purchased a higher level of service ($15.95) at the time of the first log in. (PX 49 at IHG 3.) This higher level of service, which was purchased from Salyards' computer (MAC Address 00:21:70:A9:54:51),[FN5] assigned Salyards' computer an IP address of 64.186.161. *12*. (PX 38 at IHG 3 (emphasis added).) Also during the time of the first log in, another room at the Mark Hopkins Hotel—which Salyards paid for—used a computer with a different MAC Address (00:21:9B:E1:BD:5F) to purchase a lower level of internet service ($12.95) that did not assign a specific IP address. (PX 38 at IHG 7.) The second log-in on April 23, 2009, 10:15 p.m. PDT, occurred when a lower level of service ($12.95) was purchased through Salyards' computer (MAC Address 00:21:70:A9:54:51). (*See* PX 38 at IHG 4.)

> FN5. A MAC address is a physical address associated with a computer's unique network adaptor. (Tr. 193:9–10.)

Obuchowski acknowledges that the IP address 64.186.161.12, which was assigned to Salyards when he purchased a higher level of internet service at the Mark Hopkins Hotel, is not reflected in the Hush logs. (Tr. 191:1–15.) He reconciles this discrepancy by explaining that, when a lower level of service is purchased, the Mark Hopkins Hotel assigns its own IP address through a public IP service; therefore, the .2 IP address reflected in the Hush logs must have been the public IP address that the Hotel assigned when the lower level of service was purchased by the non-Salyards MAC address on April 20 and by the Salyards MAC address on April 23. (Tr. 191:9–22, 240:17–241:16.)

VI. Evidentiary Hearing in January 2010

The Court held an evidentiary hearing on January 13, 2010, intended to last no more than a day and a half, but which went on for five days. At the hearing, Passlogix proffered two arguments: (1) the Hush logs, Mark Hopkins Hotel records, and other circumstantial evidence establish that Salyards committed a fraud on the court by (a) transmitting the September 3 e-mail to procure a better settlement from Passlogix and cause Passlogix commercial harm, (b) transmitting the April 13 e-mail as pretext to obtain third party discovery, and (c) orchestrating Collier's confession to writing the April 13 email; and (2) 2FA engaged in spoliation of evidence by failing to implement a litigation hold policy at the onset of this litigation, leading to the destruction of relevant documents. (Tr. 8:4–12:1.) In support of its position, Passlogix presented live testimony from Boroditsky, Manza, Scott Bonnell, and Salyards. It also presented live expert testimony from Obuchowski and Doug Brush, who the Court qualified on a limited***393** basis as an expert in computer forensics. (Tr. 481:8–482:1.) As a remedy for Salyards' alleged fraud on the court, Passlogix asks the Court to dismiss 2FA's pleadings and award Passlogix costs for its investigation into the authorship of the e-mails. (Mem. 35.) Passlogix also requests an adverse inference, preclusion, and costs for 2FA's alleged spoliation of evidence. (*Id.* 33–34.)

2FA asserts the following claims and affirmative defenses: (1) Collier's admission to writing the April 13 e-mail and spoofing Salyards' IP address subsequent to sending that e-mail vindicates Salyards; (2) there is circumstantial evidence pointing to Robinson as the author of the September 3 e-mail; (3) Passlogix, not 2FA, committed a fraud on the court by submitting both anonymous e-mails

to the Court with a bad faith intent to delay adjudication on the merits; and (4) no spoliation of evidence occurred because the documents that Salyards did not preserve were not evidence when they were deleted and, even if they were evidence, they would have been helpful to 2FA, not Passlogix. (Opp'n Mem. 1, 5, 8, 29.) 2FA presented live testimony from Cuttill and Boroditsky, in addition to Dr. Alan Perlman, from whom the Court heard testimony but declined to qualify as an expert in linguistics. (Tr. 259:14–260:5, 261:1–8.) 2FA asks the Court to dismiss Passlogix's claims with prejudice and award 2FA relief, including but not limited to reimbursement for the costs incurred to defend itself and Salyards, which, as of January 21, 2010, totaled approximately $200,000. (Opp'n Mem. 35; Tr. 569:10–18.)

DISCUSSION

The Court first addresses whether either party has established that its adversary committed a fraud on the court. Then the Court turns to Passlogix's allegation that 2FA engaged in the spoliation of evidence.

I. Fraud on the Court

Passlogix fails to establish that Salyards committed a fraud on the court. Likewise, 2FA fails to establish that Passlogix committed a fraud on the court and, therefore, is not entitled to amend its counterclaims to assert a malicious prosecution claim against Passlogix. In reaching these conclusions, the Court first addresses the legal standard for fraud on the court. Then the Court explains why each party has failed to demonstrate that its adversary committed a fraud on the Court.

A. Legal Standard

[1][2][3] A fraud on the court occurs where it is established by clear and convincing evidence "that a party has sentiently set in motion some unconscionable scheme calculated to interfere with the judicial system's ability impartially to adjudicate a matter by ... unfairly hampering the presentation of the opposing party's claim or defense." *McMunn v. Mem'l Sloan–Kettering Cancer Ctr.*, 191 F.Supp.2d 440, 445 (S.D.N.Y.2002) (quoting *Aoude v. Mobil Oil Corp.*, 892 F.2d 1115, 1118 (1st Cir.1989)); *see also Hargrove v. Riley*, No. 04 Civ. 4587, 2007 WL 389003, at *11, 2007 U.S. Dist. LEXIS 6899, at *36 (E.D.N.Y. Jan. 31, 2007); *Shangold v. Walt Disney Co.*, No. 03 Civ. 9522, 2006 WL 71672, at *4 (S.D.N.Y. Jan. 12, 2006); *Intelli–Check, Inc. v. TriCom Card Techs., Inc.*, No. 03 Civ. 3706, 2005 WL 3533153, at *11 (E.D.N.Y. Dec. 22, 2005); *Scholastic, Inc. v. Stouffer*, 221 F.Supp.2d 425, 439 (S.D.N.Y.2002). The essence of fraud on the court is "when a party lies to the court and his adversary intentionally, repeatedly, and about issues that are central to the truth-finding process." *McMunn*, 191 F.Supp.2d at 445. ***394** Fraud on the court, therefore, does not merely "embrace any conduct of an adverse party of which the court disapproves;" rather, it "embrace[s] only that species of fraud which does or attempts to, defile the court itself." *Kupferman v. Consol. Research & Mfg. Corp.*, 459 F.2d 1072, 1078 (2d Cir.1972) (Friendly, C.J.) (citation and internal quotation marks omitted) (discussing fraud on the court in the context of a Rule 60(b) motion). Consequently, "an isolated instance of perjury, standing along, will not constitute a fraud upon the court." *McMunn*, 191 F.Supp.2d at 445; *see also Jung v. Neschis*, No. 01 Civ. 6993, 2009 WL 762835, at *21 (S.D.N.Y. Mar. 23, 2009); *Skywark v. Isaacson*, No. 96 Civ. 2815, 1999 WL 1489038, at *14 (S.D.N.Y. Oct. 14, 1999). "Rather, fraud upon the court 'occurs where a party has acted knowingly in an attempt to hinder the fact finder's fair adjudication of the case and his adversary's defense of the action.' " *McMunn*, 191 F.Supp.2d at 445 (quoting *Skywark*, 1999 WL 1489038, at *14).

[4] The Court has inherent authority "to conduct an independent investigation in order to determine whether it has been the victim of fraud." *Chambers v. NASCO, Inc.*, 501 U.S. 32, 44, 111 S.Ct. 2123, 115 L.Ed.2d 27 (1991); *see also Universal Oil Prods. Co. v. Root Ref. Co.*, 328 U.S. 575, 580, 66 S.Ct. 1176, 90 L.Ed. 1447 (1946). "Because of their very potency, inherent powers must be exercised with restraint and discretion." *Chambers*, 501 U.S. at 44, 111 S.Ct. 2123. The Court's inherent powers serve "to do whatever is reasonably necessary to deter abuse of the judicial process and assure a level playing field for all litigants." *Shangold*, 2006 WL 71672, at *4.

[5][6] If it is shown by clear and convincing evidence that a party perpetrated a fraud on the Court, the Court may consider the following five factors in determining an appropriate sanction: (i) whether the misconduct was the product of intentional bad faith; (ii) whether and to what extent the misconduct prejudiced the injured party; (iii) whether there is a pattern of misbehavior rather than an isolated instance; (iv) whether and when the misconduct was corrected; and (v) whether further misconduct is likely to occur in the future. *See Shangold,* 2006 WL 71672, at *4; *Intelli–Check,* 2005 WL 3533153, at *11; *Scholastic,* 221 F.Supp.2d at 444; *McMunn,* 191 F.Supp.2d at 461. When faced with a fraud on the court, "[t]he available sanctions at a court's disposal ... range from the issuance of a jury charge on falsehoods under oath, to the imposition of attorney's fees occasioned by the conduct in question, and finally to the entry of judgment against the offending party." *Skywark,* 1999 WL 1489038, at *14 (internal citations omitted).

B. Application

First, the Court explains the showing required to establish a fraud on the court claim. Next, the Court applies the fraud on the court standard in holding that neither Passlogix nor 2FA has demonstrated that its adversary committed a fraud on the court by its conduct in this litigation.

1. 2FA Misstates the Fraud on the Court Standard

2FA insists that "[i]t is essential—it is the foundation of fraud on the court—that the party accused first submits evidence, evidence that eventually is found to be fraudulent or fabricated. Otherwise there cannot possibly be fraud on the Court." (Opp'n Mem. 4.) 2FA argues that although it wrote a letter to Magistrate Judge Dolinger dated September 14, 2009, bringing the anonymous misappropriation claims in the September 3 e-mail to Judge Dolinger's***395** attention, it never attached the September 3 e-mail and, thus, did not "submit" evidence. (*Id.*) Instead, 2FA states that it was Passlogix that "submitted" both anonymous e-mails by attaching them as exhibits to Passlogix's October 27, 2009 letter to this Court. (*Id.* 1.) Moreover, 2FA asserts that neither anonymous e-mail constitutes "evidence" under the Federal Rules of Evidence. (*Id.* 4.) Since Passlogix cannot make this threshold showing, 2FA insists that Passlogix's fraud on the court allegation fails as a matter of law. (*Id.*)

2FA misinterprets the requirements necessary to establish a fraud on the court. 2FA provides the holdings of five fraud on the court cases, which, as 2FA states correctly, sanctioned parties for "submitting" actual "evidence" to the court. *See Hargrove,* 2007 WL 389003, at *3, *11, 2007 U.S. Dist. LEXIS 6899, at *11, *38 (dismissing plaintiff's claims with prejudice where plaintiff provided fraudulent documents to defendants during discovery and attached said documents as exhibits to his complaint and his affidavit in opposition to defendant's motion for summary judgment); *Shangold,* 2006 WL 71672, at *5 (dismissing plaintiff's misappropriation case with prejudice and awarding costs and attorneys' fees to defendants where plaintiffs "fabricated evidence and manipulated the judicial process"); *Scholastic,* 221 F.Supp.2d at 444 (granting plaintiff's motion for sanctions where defendant "perpetuated a fraud on the Court through her submission of fraudulent documents [as exhibits to her counterclaims] as well as her untruthful testimony"); *McMunn,* 191 F.Supp.2d at 452, 454, 462 (dismissing plaintiff's action with prejudice and awarding monetary sanctions where plaintiff perpetuated a fraud on the court by tampering with evidence and repeatedly providing false testimony); *Cerruti 1881 S.A. v. Cerruti, Inc.,* 169 F.R.D. 573, 574 (S.D.N.Y.1996) (granting plaintiffs' motion to strike defendants' answer and all but one counterclaim and awarding plaintiffs costs and attorneys' fees where defendants, through their principal, fabricated evidence and offered false testimony). As these cases demonstrate, submitting false evidence to a court may rise to the level of a fraud on the court; however, it is not the only way to commit a fraud on the court. A fraud on the court occurs where a party: (1) "improperly influence[es] the trier," *McMunn,* 191 F.Supp.2d at 445 (citation and internal quotation marks omitted); (2) "unfairly hamper [s] the presentation of the opposing party's claim or defense," *Id.* (citation and internal quotation marks omitted); (3) "lies to the court and

his adversary intentionally, repeatedly, and about issues that are central to the truth-finding process," *Id.;* or (4) "knowingly submit[s] fraudulent documents to the Court," *Scholastic*, 221 F.Supp.2d at 443.

Given this clarification, the Court holds that even if the anonymous e-mails are not "evidence" under the Federal Rules of Evidence and 2FA did not "submit" the e-mails to the Court, these two facts do not obviate the need for the Court to determine whether 2FA engaged in an "unconscionable scheme" to interfere with the adjudication of this case by unfairly hampering Passlogix's claims or defenses or by lying to the court and Passlogix about issues central to the case. *See Hargrove*, 2007 WL 389003, at *11, 2007 U.S. Dist. LEXIS 6899, at *36; *Scholastic*, 221 F.Supp.2d at 439; *McMunn*, 191 F.Supp.2d at 445; *Skywark*, 1999 WL 1489038, at *14. Below, the Court analyzes whether a fraud on the court has been established.

2. Passlogix has Failed to Establish that Salyards Committed a Fraud on the Court

Passlogix has failed to present clear and convincing evidence that Salyards authored ***396** the April 13 and September 3 e-mails and used them to commit a fraud on the Court. Below, the Court first addresses the testimony offered by Passlogix's expert, Obuchowski, and determines to what extent to credit his conclusions. Then, the Court analyzes the evidence that Passlogix submits in support of its claim, and explains why, in totality, the evidence does not meet Passlogix's burden of proof.

a. *Expert Testimony by Obuchowski*

[7][8][9] "[A]n expert testifying on the basis of experience may form his conclusions by applying his extensive experience to the facts of the case." *In re Methyl Tertiary Butyl Ether Prods. Liab. Litig.*, No. M21–88, 2008 WL 1971538, at *10 (S.D.N.Y. May 7, 2008); *see also Kumho Tire Co., Ltd. v. Carmichael*, 526 U.S. 137, 152, 119 S.Ct. 1167, 143 L.Ed.2d 238 (1999). Where, as here, an expert's "qualifications and testimony rest on his ... experience and not on scientific, mathematical or social science studies or calculations, ... [the expert] must ... apply his experience to the facts using the same intellectual rigor a professional [in his field] would use in practice." *In re Methyl*, 2008 WL 1971538, at *10; *see also Kumho*, 526 U.S. at 152, 119 S.Ct. 1167 ("[A]n expert, whether basing testimony upon professional studies or personal experience, employs in the courtroom the same level of intellectual rigor that characterizes the practice of an expert in the relevant field."). Contentions that the expert's " 'assumptions are unfounded go to the weight, not the admissibility, of the testimony.' " *In re Methyl*, 2008 WL 1971538, at *12 (quoting *Boucher v. U.S. Suzuki Motor Corp.*, 73 F.3d 18, 21 (2d Cir.1996)); *see also McCullock v. H.B. Fuller Co.*, 61 F.3d 1038, 1044 (2d Cir.1995) (McLaughlin, J.) (stating, with respect to a scientific expert, that "[d]isputes as to the strength of [the expert's] credentials, faults in his use of ... [a particular] methodology, or lack of textual authority for his opinion, go to the weight, not the admissibility, of his testimony").

[10][11] Where, as here, the Court acts as the trier of fact, it uses "the discretion given to it ... [to] parse and evaluate the evidence ... for its weight and worth." *United States v. Alcan Aluminum Corp.*, No. 03 Civ. 0765, 2006 WL 5278224, at *1, 2006 U.S. Dist. LEXIS 39042, at *4 (N.D.N.Y. June 9, 2006); *see also New York v. Solvent Chem. Co., Inc.*, No. 83 Civ. 1401C, 2006 WL 2640647, at *1–2, 2006 U.S. Dist. LEXIS 65595, at *4 (W.D.N.Y. Sept. 14, 2006) ("[T]he concerns expressed in *Daubert* and *Kumho Tire* about the need for the trial court to guard against the admission of unreliable scientific or technical evidence are not implicated in a non-jury trial."). Pursuant to its role as factfinder, the Court may credit an expert's testimony in whole or in part, regardless of whether another expert is called in rebuttal. *See Giles v. Rhodes*, 171 F.Supp.2d 220, 226, 230 (S.D.N.Y.2001) (denying plaintiff's motion for a new trial where jury had the power to refuse to credit plaintiff's expert's opinion, even though another expert was not called to rebut it); *accord* Leonard B. Sand, et al., 4 Modern Federal Jury Instructions–Civil ¶ 76–9 cmt. ("[E]xpert testimony is designed to *assist* the jury to reach an independent decision on the facts, and ... is not a *substitute* for the jury's common sense evaluation of the evidence." (emphasis in original)).

While the Court credits much of Obuchowski's expert

testimony, it declines to credit some of his ultimate conclusions. The Court credits Obuchowski's conclusions that, in his experience, (1) he has not come across software capable of doing the kind of IP spoofing that is alleged here, and (2) the MAC IP Change Program is incapable of doing the kind of IP spoofing ***397** that is alleged here. However, the Court declines to credit Obuchowski's broader conclusion that spoofing an IP address assigned by an internet service provider ("ISP")—the type of spoofing that is alleged to have been done here—is technologically impossible. (*See* Passlogix's Post–Hearing Reply Mem. ("Reply Mem.") 4 ("Obuchowski's conclusions are *unrebutted* that ... IP address spoofing is not technologically feasible here ...." (emphasis in original)).) This conclusion is contradicted by Obuchowski's initial declaration, which states that "spoof[ing] the IP address in order for it to appear as 70.114.246.62 is extremely difficult and highly improbable," rather than impossible. (PX 36 ¶ 14.) Similarly, at the preliminary hearing, Obuchowski equivocated about whether it is possible to spoof an IP address assigned by an ISP. (*See* Prelim. Hr'g Tr. 39:13–17 ("[B]ecause an IP address is already assigned by an Internet service provider to a company or to an individual, *...it's very difficult, if at all,* to spoof that because that IP address is assigned." (emphasis added)).) Obuchowski's more nuanced conclusion that "IP spoofing of an [ISP] IP address is not possible *to the extent of being undetected* " also is problematic because Obuchowski does not explain what kind of "inconsistencies" would appear in the "email message headers." (PX 36 ¶ 15 (emphasis added).) Obuchowski states that "jumps" in the e-mail headers are "one attribute" that "would lead [one] to believe that ... potential IP spoofing existed"; however, he does not explain what a "jump" might look like in the e-mail headers here or whether there are other indicia of spoofing that he considered and concluded did not exist in the e-mail headers. (Prelim. Hr'g Tr. 40:12–14.) Also, there is personal experience testimony contradicting Obuchowski's conclusion that spoofing an IP address assigned by an ISP is technologically impossible, albeit by interested lay parties. Both Salyards and Cuttill testified to having spoofed IP addresses in their personal experience and Cuttill specifically testified to spoofing a public IP address assigned by an ISP. (Tr. 389:3–11, 390:13–392:3, 565:9–567:17, 589:25–591:25.)

The Court also finds Obuchowski's conclusions regarding how the Mark Hopkins Hotel assigns and routes IP addresses inconclusive at best, as Obuchowski admits that his conclusions are not based on personal knowledge about the Hotel's IP address routing practices. (*See* Tr. 213:20–21 ("How the hotel is assigning [its] IP addresses and their uses that they use them for, I do not know."), 618:5–11 (stating that "Mark Hopkins did not supply information in the records" regarding its IP address routing practices and that he is "not sure exactly how Mark Hopkins is routing traffic").)

While the Court does not form its own judgment regarding whether spoofing an IP address assigned by an ISP is technologically feasible, it holds that Obuchowski's equivocating statements and inconsistencies noted elsewhere in this decision lead the Court to decline to credit his conclusion that such spoofing is impossible.

b. *April 13 E-mail*

The substance of the April 13 e-mail primarily relates to Wal–Mart, a Passlogix customer with whom Passlogix was finalizing an agreement. (PX 2; Mem. 16.) The e-mail also references Oracle, as well as an executive, Adnan, from Deloitte & Touche—all companies that 2FA was seeking to subpoena in connection with the underlying litigation. (PX 2; Mem. 16.) The anonymous author of the April 13 e-mail claims that Passlogix is in jeopardy of losing the Wal–Mart account because a certain Passlogix executive was leaking Passlogix's information. (PX 2.) The e-***398** mail also references 2FA and claims that Adnan "has a lot of respect for [Salyards]" and states that "[h]opefully Passlogix's legal issues will not spill over to [the Wal–Mart] account." (*Id.*) Passlogix considered the April 13 e-mail when investigating the September 3 e-mail because the April 13 e-mail is "the only other anonymous, Hush email that Passlogix management has ever received." (Mem. 3.) Passlogix's stated purpose in introducing the April 13 e-mail "is to reveal a pattern of misconduct, and thereby corroborate Salyards' culpability for the critical September 3 Email." (*Id.* 15.)

i. *Evidence Presented by Passlogix*

Passlogix's strongest evidence that Salyards authored the April 13 e-mail are the logs that Passlogix subpoenaed from Hush, which indicate that the April 13 e-mail was sent from 2FA's office IP address. (*See* PX 49.) Passlogix contends that "the April 13 Hush Log reflects IP addresses that notably shift from Salyards' office to his home in Austin; from Austin to a specific San Francisco hotel, where he stayed while attending a conference; and then back to Austin." (Mem. 17.) Passlogix notes that each log-in to Hush syncs "precisely to Salyards' moving whereabouts": from work (April 13, 6:15 p.m. CDT), to home (April 13, 10:38 p.m. CDT), to work (April 14, 3:19 p.m. CDT), to work again (April 15, 8:58 p.m. CDT), to work again (April 16, 10:29 a.m. CDT), to work again (April 17, 10:31 a.m. CDT), to San Francisco (April 20, 10:30 a.m. PDT), to San Francisco again (April 23, 10:15 p.m. PDT), and back to work (April 27, 1:26 p.m. CDT). (Mem. 17–18; PX 49.) Passlogix insists that "the likelihood that a spoofer would be able to accurately capture the [se] different IP addresses ... is not credible." (Mem. 18.)

Passlogix points to timing and motive for corroboration, stating that Salyards sent the April 13 e-mail to Boroditsky and Gillespie to gain leverage in a discovery dispute in which 2FA sought to serve third-party subpoenas on business entities with whom Passlogix has commercial relationships. (*See* Mem. 15–16.) Passlogix contends that the unrebutted testimony of its expert, Obuchowski, confirms that the Hush logs and the records from the Mark Hopkins Hotel provide dispositive evidence that Salyards authored the April 13 e-mail. (*See* Mem. 2–3; PX 36, 38, & 44; Tr. 153:9–13.)

Passlogix also presents evidence contradicting Collier's confession to sending the April 13 e-mail. Obuchowski states that Collier did not send the April 13 e-mail because Collier was incorrect about when the April 13 Hush account was created and about the password he used to create it. (Tr. 165:4–166:25, 168:14–20; PX 41.) Obuchowski also states that the MAC IP Change program that Collier recalled using to conceal his IP address "does not have that capability." (Tr. 164:7–11.) Moreover, Obuchowski concludes "that there is no evidence of IP spoofing as being claimed" because the spoofing that 2FA alleges would have left evidence in the header of the April 13 e-mail, which is not present. (Tr. 153:9–13, 170:15–18; PX 36 ¶ 15.)

To further discredit Collier's admission, Passlogix points to Collier's activities during the time period when the April 13 e-mail was sent. First, Doug Brush, who the Court qualified on a limited basis as an expert in computer forensics (Tr. 481:8–482–1), testified that on April 13, 2009, between 3:25 p.m. and 4:55 p.m. CDT, when Collier claims to have been at 2FA's office, there is evidence of computer user activity on Collier's work laptop under his username, including a printer installation. (Tr. 482:17–21; PX 55.) Brush also found evidence of web browsing on Collier's work ***399** laptop during this time period. (Tr. 483:19–484:4.) Second, Passlogix contends that Collier was e-mailing a Passlogix employee, Jennifer Kilmer, through his Passlogix e-mail account during the time that he claims to have been at 2FA's office. (Tr. 49:16–51:11; PX 56.) Third, Passlogix argues that Collier's phone records indicate that Collier was on a thirteen-minute phone call with Salyards on April 13 between 3:02 and 3:15 p.m. CDT, which contradicts Cuttill's testimony that Collier arrived at 2FA's office around 3:00 p.m. and that the two spoke for "about ten minutes or less." (Tr. 594:9–25; PX 45 at CC10, Item 212.) Fourth, Passlogix argues that Collier would not have had enough time to set up the Hush account and send the e-mail because Collier was on a sixteen-minute phone call with a Passlogix employee, Stephan Wardell, during the time frame that the Hush account was being set up. (Tr. 167:1–168:13; PX 45 at CC10, Item 213.)

ii. *Evidence Rebutted by 2FA*

2FA rebuts Passlogix's evidence that Salyards authored the April 13 e-mail. First, 2FA maintains that the mere content of the April 13 e-mail, which discloses a business opportunity with Wal–Mart that 2FA was pursuing as a competitor to Passlogix, eliminates the possibility that Salyards—the President, CEO, and co-founder

of 2FA—would have sent it to Passlogix. (Opp'n Mem. 9; Tr. 385:22–25.)

Second, 2FA contends that Collier's sworn confession to writing the April 13 e-mail discredits any suggestion that Salyards authored it. (Opp'n Mem. 9.) Collier's motive for sending the April 13 e-mail supports this conclusion. Collier testified—and Cuttill confirmed—that he learned about 2FA competing for the Wal–Mart opportunity from Cuttill during a visit to 2FA's office. (Collier Dep. 108:15–110:15; Tr. 536:22–537:16.) Collier explained that, prior to his employment at Passlogix, he "spent and invested a lot of time and energy into the Wal–Mart account" and felt that the "deal was extremely important to the success of Passlogix," especially after just transitioning from a company that went out of business, so he sent the e-mail to "warn [ ] Passlogix about threats at Wal–Mart." (Collier Dep. 61:15–16, 76:20–77:13).

Third, 2FA refutes Obuchowski's conclusions regarding the implausibility of IP spoofing. Collier testified that he is familiar with Hush and IP spoofing. (*See* Collier Dep. 107:8–14 (stating that although he had "not used Hush in years" prior to sending the April 13 e-mail, he has used Hush "three or four times before ... to send secure e-mail.").) Collier explained that he was aware that Hush tracks the IP addresses that interact with it

> [b]ecause it's kind of the second half of the equation.... [A]nyone in the security industry I hope would know that. an anonymous e-mail service with the big disclaimer that says it at the bottom of their home page before you log on, you have to know that you're not truly anonymous unless you change that [IP] address.

(*Id.* 107:22–108:10.) Collier testified that he did not spoof 2FA's IP address when he sent the April 13 e-mail since he sent the e-mail from 2FA's office network. (Collier Dep. 62:4–11, 76:15–19, 83:11–14, 84:6–8.) Obuchowski acknowledges that if Collier sent the April 13 e-mail from 2FA's network, "then 2FA's IP address would appear in the logs." (Tr. 231:22–25.) To explain why the Hush logs appear to track Salyards' movement from work, to home, to the Mark Hopkins Hotel, 2FA points to Collier's testimony, which explains that in signing on to Hush following the April 13 e-mail, Collier used an IP address "from ***400** the e-mail header properties of an e-mail that [he] had from 2FA." (Collier Dep. 87:16–18, 70:12–21.) When asked whether he used the same IP address every time he logged on to Hush, Collier responded that he "was less interested in the exact numbers than ... that it came from the same source, which would have been, unfortunately, Greg Salyards [ ] at the time." (*Id.* 87:21–88:1.) Collier then reiterated that he used "the same IP address or range of IP addresses based upon a 2FA e-mail." (*Id.* 88:18–89:1.) Collier's only stated reason for using Salyards' IP address was that he sent the April 13 e-mail from 2FA's "IP address the first time and just to maintain ... the same thing. It wasn't relevant. It didn't seem relevant." (*Id.* 88:2–12.) Cuttill also suggests that Collier may have had a typo when spoofing Salyards' Mark Hopkins Hotel IP address ending in .12, resulting in the .2 IP address logged by Hush. (Tr. 602:16–603:2.) Moreover, Salyards challenges Passlogix's assertion that the Hush logs track his "exact geographical location," (Mem. 18), since Passlogix has not introduced evidence that Salyards actually was at home or at his office during the times captured by Hush. For instance, the Hush log from April 15, 8:58 p.m. CDT indicates that the account was accessed from Salyards' work IP address at a time when, if compared to the other work entries captured by Hush, Salyards would have been at home. (PX 49.)

With respect to the gaps in Collier's testimony, 2FA contends that Collier said that he did not remember if the Hush password he provided Passlogix was "exactly the password [he] used, because [he had not] been there for months now." (Collier Dep. 85:18–19.) Collier also said that he "can't be sure" that the MAC IP Change program was indeed the program he used to spoof Salyards' IP address to log on to Hush after April 13. (*Id.* 86:23–25.) Collier does not have the laptop that he used to send the April 13 e-mail to corroborate his sending of the email because he "decommissioned" it and gave it "to a friend in need." (PX 45 at CC–000A; *see also* Collier Dep.

108:11–14.)

Fourth, 2FA insists that the Mark Hopkins Hotel records exonerate Salyards since they show a different IP address than the one indicated on the Hush logs. (Opp'n Mem. 18.) Specifically, the Mark Hopkins Hotel records indicate that, over the course of Salyards' five-night stay, two levels of internet services were purchased for the rooms Salyards paid for: a higher level, which assigned the guest a specific IP address, and a lower level, which did not assign a specific IP address. (PX 38.) When the higher level of service was purchased from April 20—April 23, 2009, the rooms that Salyards paid for were assigned two IP addresses: 64.186.161.12 and 64.186.161.57. (*Id.*) The Hush logs, however, document two log-ins to Hush from a slightly different IP address—64.186.161.2–on (1) April 20, 10:30 a.m. PDT, and (2) April 23, 10:15 p.m. PDT. (PX 49.) 2FA claims that the Hush logs exonerate Salyards because the Mark Hopkins Hotel never assigned Salyards an IP address ending in ".2"—the IP address the Hush logs captured. (Opp'n Mem. 18.)

Obuchowski attempts to reconcile this inconsistency by insisting that "[t]he IP address of .2 and .12 both resolve back to the Mark Hopkins Hotel." (Tr. 213:9–10.) Obuchowski states that it is common for hotels to have multiple IP addresses "facing the Internet," such that when a guest purchases a lower level of internet service that does not assign a particular IP address, the guest is routed to one of the hotel's available IP addresses—in this case, the .2 IP address that Hush captured. (Tr. 191:9–22, 240:17–241:16, 614:3–15.) Obuchowski admits, however, that his ***401** explanation is no more than a guess that is not grounded in the facts or evidence presented in this case. (*See* Tr. 213:20–21 ("How the hotel is assigning [its] IP addresses and their uses that they use them for, I do not know.").) When asked whether there was "any evidence from Mark Hopkins that indicates that traffic in this particular situation was routed outward using a different IP address than .2, or .12," Obuchowski acknowledged that "Mark Hopkins did not supply [this] information in the records" and that he is "not sure exactly how Mark Hopkins is routing traffic other than that they are using the .12 for web-based traffic." (Tr. 618:1–11.) While Obuchowski's theory is grounded in his "experience in conducting hundreds of investigations, including several hotels," none of those hotels includes the Mark Hopkins. (Tr. 618:6–7.) 2FA also challenges Obuchowski's "re-routing" theory by pointing to several e-mails from Salyards to Cuttill between April 20 and April 22, 2009, all originating from Salyards' Mark Hopkins Hotel IP address ending in .12, not .2. (DX 7 at 11015–20; Tr. 598:21–600:17.)

Fifth, 2FA refutes Passlogix's contention that Collier was engaged in activities that would have prevented him from sending the April 13 e-mail. With respect to evidence of Collier installing a printer on his Passlogix laptop while he claims to have been at 2FA, Collier made clear that he sent the April 13 e-mail from his personal, not Passlogix, laptop. (Collier Dep. 62:6–8; Opp'n Mem. 21.) The fact that a printer was being installed and websites were visited on Collier's work computer at the time Collier claims to have been at 2FA does not mean that Collier could not have sent the April 13 e-mail from 2FA's office using his personal computer. While Passlogix contends that Collier was e-mailing Jennifer Kilmer from Collier's Passlogix e-mail account at the time he claims to have been at 2FA's office writing and transmitting the April 13 e-mail, Cuttill clarified—and the Court agrees—that Collier's e-mail correspondence with Kilmer occurred between 1:23 p.m. CDT and 2:27 CDT, which was before Collier's stated arrival at 2FA's offices around 3 p.m. (Tr. 49:16–51:11, 529:23–531:11; PX 56.) With respect to Collier's thirteen-minute phone call with Salyards from 3:02 to 3:15 p.m. CDT, Cuttill's testimony that Collier arrived at 2FA's office around 3:00 p.m. CDT, "give or take maybe 15 minutes," leaves open the possibility that Collier arrived around 2:45 p.m. and finished his ten-minute (or so) conversation with Cuttill before beginning the call with Salyards. (Tr. 594:10–25; PX 45 at CC10, Item 212.) With respect to evidence that Collier was on the phone with Wardell during the time he claims to have been at 2FA, besides the prospect of multi-tasking, there is a seven-minute gap between when the Hush account was set up at 3:32 p.m. CDT and the start of Collier's call with Wardell at 3:39 p.m. CDT, leaving sufficient time to draft a

two-paragraph e-mail. (PX 45 at CC10, Item 213; Tr. 221:11–24.) Moreover, the call ended at 3:55 p.m. CDT, leaving four more minutes before the e-mail was transmitted. (PX 45 at CC10, Item 213; Tr. 222:6–12.)

iii. *Passlogix Fails to Present Clear and Convincing Evidence that Salyards Authored the April 13 E-mail*

[12] After reviewing all of the evidence in this case, including Collier's three-hour videotaped deposition, the Court holds that Passlogix has not presented clear and convincing evidence that Salyards authored the April 13 e-mail. Virtually every piece of evidence Passlogix presents is rebutted by 2FA. Importantly, the Court finds Collier's admission to authoring the April 13 ***402** e-mail credible.[FN6] Collier's motive for sending the April 13 e-mail is logical, he matches the profile of the author,[FN7] and his testimony regarding his subsequent log-ins is corroborated by the Hush logs. [FN8] Although some inconsistencies remain with respect to Collier's confession, they do not amount to clear and convincing evidence that Salyards authored the e-mail. For instance, Collier stated that he set up the Hush account "a few days before the [April 13] e-mail was sent," yet the Hush logs indicate that the account was set up just twenty-seven minutes before the e-mail was sent. (Collier Dep. 84:10–12, 85:20–86:1; *see also* PX 44 ¶ 6; PX 49.) Also, the password that Collier provided did not match the password used to access Hush. (*See* Collier Dep. 84:17–85:19; PX 41 & 44 ¶ 5.) However, Collier admitted that he was not sure whether the password he provided was correct and, because there are no records from Hush indicating what the actual password was, the Court does not know whether the password Collier offered was close to the actual password used. (Collier Dep. 85:17–19; PX 41.) In any event, Collier's inaccuracies about the date the Hush account was created and the password he used to create the account do not convince the Court that Collier is lying. For example, Passlogix's own expert admitted that he too could not recall when he set up his more recent Hush test account and what password he assigned to it. (Tr. 235:24–236:5.)

FN6. Passlogix claims that Collier's confession is not credible because Collier previously "disavow[ed] any knowledge of the emails to Passlogix and its lawyers." (Mem. 20.) However, prior to his December 2, 2009 deposition, Passlogix never asked Collier directly whether he sent the April 13 e-mail. (Collier Dep. 80:8–82:5.)

FN7. The April 13 e-mail, which was sent on a Monday, refers to the author being on a "call this morning." (PX 2.) Boroditsky testified that Passlogix has a weekly sales call on Mondays. (Tr. 72:13.) While Boroditsky did not know whether Collier was on the call that Monday, April 13, he acknowledged that Collier "has been on those calls." (Tr. 72:17–22.) Salyards, on the other hand, was not supposed to be on those calls. (Tr. 72:15–16.) Boroditsky also stated that the topic of Oracle being brought into the Wal–Mart account "could have been raised" during those Monday sales calls, further linking Collier to the April 13 e-mail. (Tr. 72:23–25.)

FN8. Collier testified that after sending the April 13 e-mail, he logged into Hush "[s]ix, maybe seven times" and that the last time he accessed the Hush account "may have been two weeks after [the April 13 e-mail] was sent." (Collier Dep. 86:2–4, 89:2–6.) This testimony largely is consistent with the Hush logs, which indicate nine log-ins to Hush after the April 13 e-mail was sent and show a final log-in on April 27, 2009, fourteen days after the April 13 e-mail was sent. (PX 49.)

As discussed earlier, the Court does not credit Obuchowski's conclusion that the kind of IP spoofing at issue here is technologically impossible. *See supra.* Therefore, given Collier's equivocation about the program that he used to spoof Salyards' IP address, Obuchowski's testimony regarding the MAC IP Change program's inability to spoof IP addresses to the degree done here—which the Court credits—is not dispositive of the fact that IP spoofing could not, and did not, happen. (Collier Dep. 86:23–25;

Tr. 242:5–11; PX 44 ¶¶ 3–4.)

With respect to how Collier spoofed an IP address similar to the one that the Mark Hopkins Hotel assigned to Salyards, Collier states that the only way he could have used an IP address similar to that of the Mark Hopkins Hotel is if he copied it from an e-mail header that Salyards sent to Collier from the Hotel. (Collier Dep. 93:24–94:1.) In an affidavit submitted to the Court, Salyards states that on April 19, 2009, he sent an e-mail to Collier "from the ***403** Mark Hopkins hotel upon [his] arrival in San Francisco via Outlook." (PX 43 ¶ 5(e).) If true, Salyards would have sent this e-mail using a lower level of internet service, which is the only type of internet service purchased by Salyards on April 19. (PX 38 at IHG7–8.) However, this level of internet service was linked to a computer with a MAC address different than Salyards' computer. (*Id.*) Thus, there is a gap in the record concerning how Collier was able to spoof Salyards' IP address from the Mark Hopkins Hotel using the April 19 e-mail that Salyards allegedly sent. The record also is bare with respect to whether Salyards and Collier may have communicated through remote means, such as a blackberry device, and, if so, what IP address would appear in the e-mail headers of those e-mails. These remaining questions, however, do not amount to the clear and convincing evidence that Passlogix needs to present to prove that Salyards wrote the April 13 e-mail and used it in an attempt to commit a fraud on the Court.

c. *September 3 E-mail*

[13] The September 3 e-mail, which was sent the day after Passlogix submitted its opposition to 2FA's motion for a preliminary injunction, accuses Passlogix of using 2FA's and Imprivata's intellectual property in violation of "contractual and ethical obligations." (PX 1.) The anonymous author claims to have transitioned to Passlogix "earlier this year" and to have over fifteen years of development experience. (*Id.*) The e-mail contains two attachments consisting of Passlogix's confidential technical specifications for a project under development—the dissemination of which "created a serious risk of competitive harm and lost investment for Passlogix." (Mem. 6.) Passlogix seeks sanctions for 2FA's affirmative use of the September 3 e-mail "as negotiating leverage before the settlement conferences on September 16 and October 1, 2009" and for 2FA's "interject[ing] the email into the case as pretext for demanding broad document and deposition discovery into Passlogix's operations." (*Id.*)

i. *Evidence Presented by Passlogix*

Like the April 13 e-mail, Passlogix's strongest evidence that Salyards authored the September 3 e-mail are the Hush logs, which indicate that the September 3 e-mail was sent from 2FA's office IP address (70.114.246.62). (*See* PX 48.) Passlogix also points to Obuchowski's conclusion that there is no software on the market that can be used to spoof a public IP address, including 2FA's office IP address, and that the e-mail headers from the September 3 e-mail show no indicia of spoofing. (Mem. 10; Reply 4–5; Tr. 164:6–19, 168:21–169:16, 242:12–16, 616:20–617:4, 623:17–624:2; PX 36 ¶¶ 14–15.) Passlogix states that given the timing and subject matter of the September 3 e-mail, as well as the Hush logs, it is clear that Salyards sent the email to garner a favorable settlement and to expand discovery. (Mem. 6.) Moreover, because the September 3 e-mail alleges that Passlogix misappropriates the intellectual property of third parties, attaches two proprietary Passlogix documents, and was sent to a third-party business entity that Passlogix has a commercial relationship with, Salyards clearly sought to harm Passlogix's business relations in sending the e-mail. (*Id.*) Passlogix asserts that Salyards obtained the proprietary attachments either from an anonymous e-mail that Salyards claims to have received in June or July 2009, which purportedly contained one of the attachments, or through his secretive relationship with Collier. (Tr. 137:17–22, 139:15–21, 436:14–437:2.)

***404** Passlogix insists that 2FA's suggestion that a former Passlogix employee, Joseph Robinson, authored the September 3 email is speculative and inadmissible and that the factual contentions in the September 3 e-mail belie any suggestion that Robinson was the author. (Mem. 11.) First, Passlogix states that its internal investigation concluded that that the claims in the September 3 e-mail were

false and that no individual at Passlogix, including Robinson, identified any inappropriate request to utilize intellectual property from third parties. (Tr. 35:10–21, 36:17–22; PX 34 & 35.) Second, the author of the September 3 e-mail refers to receiving a "monthly paycheck" from Passlogix, but Robinson was paid semi-weekly. (Tr. 47:24–48:6, 140:12–13; PX 1.) Third, the September 3 e-mail's author refers to having fifteen years of development experience, but Boroditsky maintains that Robinson had ten years of development experience because Robinson's first five years in the computer technology field consisted of "lesser roles that would not be claimed as software developer roles." (Tr. 48:7–11, 93:10–94:5, 101:16–102:12; PX 1.) Fourth, while the author states that he intends to stop assisting on the SAW project, Robinson continued to work on this project diligently and never raised an issue about the misuse of intellectual property. (Tr. 48:12–15, 139:5–8.) Finally, Robinson and Salyards had no communication with one another, including via e-mail, such that Robinson would have known Salyards' IP address. (Tr. 449:10–18 (Salyards testifying that he never communicated with Robinson in any way).)

Passlogix also contends that Salyards' September 3 alibi does not hold up to scrutiny. Salyards testified that he was at a restaurant with his family and friends when the September 3 email was sent, thereby refuting any claim that he authored the e-mail. (Tr. 433:8–435:19.) Three of Salyards' restaurant companions, as well as Salyards' wife, submitted affidavits and sat for depositions to confirm Salyards' whereabouts on the afternoon of September 3. (DX 1 (2FA Ltr. 10/29/09 at 4 & Ex. 2).) Passlogix, however, contends that the "recollections from these friendly witnesses ... each of whom arrived and left at different times ... are inconsistent and contradictory." (Mem. 13.) While Salyards claims that he left his office for the restaurant "at like 3:30 or so" (Tr. 434:2–9), one friend recalled Salyards arriving at "approximately 3:15" (Posey Dep. 16:15–17), another friend recalled Salyards arriving at "3:15, 3:30ish" (Dunson Dep. 14:10–12), the third friend did not "remember what time [Salyards] and his family got there" (Dismore Dep. 9:7–8), and all Salyards' wife could recall was that she arrived sometime that afternoon and believes Salyards was there already (A. Salyards Dep. 6:9–21).

ii. *Evidence Rebutted by 2FA*

2FA insists that Salyards could not have sent the September 3 e-mail because he did not have access to the proprietary Passlogix documents that were attached to it. (Opp'n Mem. 5–7.) 2FA also contends that the content of the e-mail and other corroborating evidence point to Robinson as the author. First, 2FA refers to Collier's testimony that, in June 2009, Robinson expressed concerns to him that reflect the concerns in the September 3 e-mail. (Collier Dep. 66:3–67:4, 77:17–78:24.) Specifically, Collier e-mailed Robinson on June 17, 2009, asking him to "take a quick look at the code samples that [Robinson] worked on late last year" at IdentiPHI. (DX 16 at PL96158; *see also* Collier Dep. 98:21–22.) Robinson was concerned about working on code that he did not write while at Passlogix, and raised the issue with his boss, Cory Womacks, who also hesitated about working on the code. (DX ***405** 16 at PL96148 & PL96157–58.) Collier spoke with Robinson over the phone to explain that he was asking for "development assistance for a customer that ... we were attempting to transition ... legally and ethically, from IndentiPHI to Passlogix, and [he] needed support that only the developer [Robinson] could provide." (Collier Dep. 77:21–25.) Collier says that he told Robinson to take up his issues with Boroditsky and, otherwise, abandoned his request and "never spoke to [Robinson] again." (*Id.* 98:19–99:21.) Contrary to Passlogix's assertion that 2FA relies only on Collier's speculation about Robinson being the author of the September 3 e-mail, 2FA points to an e-mail chain between Collier, Robinson, and Womacks, to corroborate Collier's version of events. (*See* DX 16 at PL96148–49 & PL96157–58.) Also, Passlogix's notes from its internal investigation indicate that both Robinson and Womacks recalled Collier requesting Robinson's help with the aforementioned code, further corroborating Collier's deposition testimony. (PX 35 at PL95991.)

Collier also testified to speaking with Robinson about Hush and about spoofing Salyards' IP address. Collier states that when Robinson expressed concern about

working on certain code, Collier suggested that Robinson raise the issue with Boroditsky or, alternatively, send an e-mail through Hush since "[t]hey won't know who you are." (Collier Dep. 68:7–16.) Importantly, Collier revealed to Robinson that he used Salyards' IP address when he sent his own anonymous e-mail, though he did not tell Robinson what that IP address was. (*Id.* 98:14–18.)

Second, 2FA states that Salyards was not in 2FA's office when the September 3 e-mail was sent and several witnesses have corroborated that he was with them at a restaurant. (Tr. 433:8–435:19; Opp'n Mem. 12.) The fact that the witnesses' testimony regarding the timeline was not identical only indicates "that nothing was rehearsed, and three of the witnesses placed Mr. Salyards at the restaurant at the crucial time, recalling what time he arrived and where they sat." (Opp'n Mem. 12.)

Third, 2FA contends that the spelling of certain words in the September 3 e-mail indicates that the author may have had a British or Canadian background, as Robinson does.[FN9] (Opp'n Mem. 15.) However, 2FA submitted dozens of Robinson's work e-mails, none of which uses the "s" spelling. (*Compare* PX 1 (anonymous author spelling "organisation" and "utilise" with an "s"), *with* DX 16 at PL96120 (Robinson spelling "organization" and "serialization" with a "z").) In any event, spelling is not dispositive of identity in this case, since one can impersonate British or Canadian spelling easily by substituting an "s" for a "z" in many common words.

FN9. At the evidentiary hearing, 2FA called Dr. Alan Perlman, a purported expert in linguistics, to testify that Salyards did not author the September 3 e-mail because the language used in the e-mail is inconsistent with his writings. Pursuant to its gatekeeping function under *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993), the Court declined to qualify Dr. Perlman as an expert and, therefore, gives no weight to his testimony in this decision. (*See* Tr. 259:14–260:5, 261:1–4.)

Fourth, 2FA maintains that additional details in the September 3 e-mail refute any claim that Salyards was the author. The author of the September 3 e-mail misspells the e-mail address of Shaun Cuttill—Salyards' long-time business partner—by using only one "t" instead of two. (Opp'n Mem. 12; Tr. 436:2–10; PX 1.) Additionally, 2FA insists that if Robinson's early technical experience is counted, he has exactly fifteen years of development experience, as stated in the September 3 e-***406** mail. (Opp'n Mem. 13; PX 1 & 21 at PL96028–30; Tr. 80:7–81:5.) Also, as the author of the September 3 e-mail represents, Robinson transitioned to Passlogix earlier in 2009 from another company. (Opp'n Mem. 13; PX 1.) There is no dispute that Robinson had access to the attachments to the September 3 e-mail, since Boroditsky confirmed that Robinson was one of four Canadian developers that Passlogix hired from IndentiPHI to work on the v-GO SAW program. (Tr. 79:1–5, 510:23–511:1; Opp'n Mem. 13; PX 1.) 2FA also contends that the anonymous author's forward-looking statement expressing an intention to leave Passlogix after securing alternative employment is consistent with Robinson's intentions. (Opp'n Mem. 14; PX 1.) 2FA states that Robinson intended to stay at Passlogix until October 1, 2009, so that he could receive his $10,000 retention bonus. (PX 21 at PL96025; Tr. 511:8–512:6; Opp'n Mem. 14.) The retention bonus benchmark and forward-looking statement also correspond with Robinson's subsequent termination on October 15, 2009, for abandoning his position due to unexcused absences. (DX 25; Tr. 515:25–516:2.) Passlogix counters that Robinson continued to assist on the SAW project until his unexcused absences in late September and that, as far as anyone knows, Robinson has not secured alternative employment. (Tr. 48:12–15.)

iii. *Passlogix Fails to Present Clear and Convincing Evidence that Salyards Authored the September 3 Email*

After reviewing all of the evidence related to the September 3 e-mail, the Court holds that Passlogix has not presented clear and convincing evidence that Salyards authored the September 3 e-mail. 2FA rebuts nearly all of Passlogix's evidence and presents a colorable coun-

ter-narrative that Robinson may have authored the September 3 e-mail. This counter-narrative is not limited to Collier's speculation, as Passlogix suggests, but rather is corroborated in part by e-mail correspondence and Passlogix's internal investigation. (*See* DX 16 at PL96148–49 & PL96157–58; PX 35 at PL95991.) While gaps undoubtedly remain regarding the identity of the author of the September 3 e-mail, 2FA does not bear the burden to prove that someone other that Salyards authored the September 3 e-mail; rather, Passlogix bears the burden to prove that Salyards was the author. Because Passlogix fails to present clear and convincing evidence that Salyards authored the September 3 email, the Court holds that Salyards did not commit a fraud on the Court.

3. 2FA Has Failed to Establish that Passlogix Committed a Fraud on the Court

2FA asserts that by alleging that Salyards committed a fraud on the court when faced with evidence to the contrary, Passlogix "fabricated accusations to interfere with the Court's ability impartially to adjudicate 2FA's counterclaims and it[s] claim of misappropriation," thereby engaging in its own fraud on the court. (Opp'n Mem. 33.) To establish its fraud on the court claim, 2FA must present clear and convincing evidence that Passlogix brought its allegation against Salyards in bad faith—that is, knowing that it was false. *See McMunn,* 191 F.Supp.2d at 445 (stating that a fraud on the court "occurs where a party has acted knowingly in an attempt to hinder ... his adversary's defense of the action") (citation and internal quotation marks omitted); *Skywark,* 1999 WL 1489038, at *14 (same); *see also Schlaifer Nance & Co., Inc. v. Estate of Warhol,* 194 F.3d 323, 338 (2d Cir.1999) ("Bad faith can be inferred when the actions taken are so completely without merit as to require the conclusion that they must have been undertaken for some improper***407** purpose.") (citation and internal quotation marks omitted). Fraud on the court will not lie where the alleged misconduct merely consists of "an advocate's view of the evidence, drawing all inferences favorable to the [client] and against the [adversary]." *Intelli–Check,* 2005 WL 3533153, at *12.

[14] 2FA has not shown that Passlogix's allegation of fraud on the Court was brought for an improper purpose. Contrary to 2FA's allegations, there is no clear and convincing evidence of an "unconscionable scheme" by Passlogix to delay the litigation; rather, Passlogix's allegations were based upon "an advocate's view of the evidence, drawing all inferences favorable to the [Passlogix] and against [Salyards]." *Id.; see also TVT Records v. Island Def Jam Music Group,* 447 F.Supp.2d 311, 315 (S.D.N.Y.2006) (holding that "even if [plaintiff] pressed this motion [for sanctions] with utmost zeal and certain aspects of it rest on grounds that are somewhat tenuous, ... the Court is not persuaded that [plaintiff's] application was frivolous, objectively unreasonable or pursued in bad faith"). Passlogix brought its fraud on the court allegation only after conducting an internal investigation and obtaining subpoenaed records from Hush, which appeared to provide objective evidence linking Salyards to both anonymous e-mails. It was not until after the Court granted the parties further discovery at the November 9 preliminary hearing that additional evidence arose challenging the conclusions drawn from the Hush logs and supporting 2FA's defense of IP spoofing. Nonetheless, even in the face of this subsequent discovery, Passlogix's continued presentation of its claim against Salyards was not "frivolous, objectively unreasonable or pursued in bad faith" because, as already discussed, the competing evidence does not conclusively support that Salyards was not the author of the e-mails; rather, it hinders Passlogix's ability to show, by clear and convincing evidence, that Salyards was the author. *TVT Records,* 447 F.Supp.2d at 314, 315 (holding that "the record lacks clear and convincing evidence to support a finding that [defendant] acted in actual bad faith at the time his ... submission was made"). The Court holds, therefore, that 2FA has failed to establish that Passlogix committed a fraud on the Court by pursuing its claims against Salyards.

4. 2FA's Request to Amend Its Complaint to Assert a Claim for Malicious Institution of Civil Proceedings is Denied

2FA requests leave to amend its counterclaims to include a claim against Passlogix for malicious institution of civil proceedings. (Opp'n Mem. 35.) 2FA states that, prior

to bringing its fraud on the court allegation against Salyards, Passlogix possessed evidence indicating that Salyards did not send either anonymous e-mail but, nonetheless, continued to pursue its claim even after obtaining further evidence during discovery that Salyards was innocent. (*Id.* 34.)

[15] Courts are instructed to "freely give leave [to amend] when justice so requires." Fed.R.Civ.P. 15(a)(2); *see also Holmes v. Grubman*, 568 F.3d 329, 334 (2d Cir.2009). Leave to amend need not be granted, however, where the proposed amendment would be futile. *See Advanced Magnetics, Inc. v. Bayfront Partners, Inc.*, 106 F.3d 11, 18 (2d Cir.1997) (Kearse, J.). In addition to futility, " '[a] district court has discretion to deny leave for ... bad faith, undue delay, or undue prejudice to the opposing party.' " *Holmes*, 568 F.3d at 334 (quoting *McCarthy v. Dun & Bradstreet Corp.*, 482 F.3d 184, 200 (2d Cir.2007)).

***408** [16] To recover on a claim of malicious prosecution under New York law, Salyards must establish that: (1) Passlogix either commenced or continued a criminal or civil proceeding against him; (2) the proceeding terminated in his favor; (3) there was no probable cause for the criminal or civil proceeding; and (4) the criminal or civil proceeding was instituted with actual malice. *See von Bulow v. von Bulow*, 657 F.Supp. 1134, 1140 (S.D.N.Y.1987); *Rosemont Enters., Inc. v. Random House, Inc.*, 261 F.Supp. 691, 695 n. 11 (S.D.N.Y.1966); *see also Russo v. New York*, 672 F.2d 1014, 1018 (2d Cir.1982), *on reh'g*, 721 F.2d 410 (2d Cir.1983); *Brady v. Penn Cent. Transp. Co.*, 406 F.Supp. 1239, 1242 (S.D.N.Y.1975). A favorable conclusion does not necessarily mean that there was no probable cause for the institution of a claim. *See Brady*, 406 F.Supp. at 1242 (holding that "[t]he fact that the indictment was discontinued against the plaintiffs does not, in and of itself, constitute a lack of probable cause for the initial arrests"). The New York Court of Appeals has stated clearly that a litigant "may act on evidence which would seem reasonably to justify making a charge, and the prosecution will not be malicious if he was mistaken about the true meaning of the evidence." *Munoz v. City of N.Y.*, 18 N.Y.2d 6, 9, 271 N.Y.S.2d 645, 218 N.E.2d 527 (1966).

[17] 2FA's request to amend its complaint to add a malicious prosecution charge is denied as futile. While Salyards can establish the first two elements of a malicious prosecution claim, he cannot establish the latter two elements of lack of probable cause and malice. As already discussed, in bringing the instant allegations, Passlogix reasonably relied on the Hush logs, which showed objective evidence that Salyards was involved in transmitting both the April 13 and September 3 e-mails. While Passlogix pressed forward notwithstanding evidence uncovered in future discovery, it did so in good faith based upon "an advocate's view of the evidence." *Intelli–Check*, 2005 WL 3533153, at *12; *see also Sauer v. Xerox Corp.*, 5 Fed.Appx. 52, 57 (2d Cir.2001) (affirming district court's denial of attorneys' fees where, "although ultimately adjudged to be without merit, [plaintiff's] suit cannot be fairly characterized as 'entirely without color and [undertaken] for reasons of harassment or delay or for other improper purposes' " (citation omitted)); *Menashe v. V Secret Catalogue, Inc.*, 409 F.Supp.2d 412, 427 (S.D.N.Y.2006) (rejecting claim for attorneys' fees where there was "nothing in [the] record to suggest that" the unsuccessful claim was brought "in bad faith, vexatiously, wantonly, or for oppressive reasons" (internal quotation marks omitted)). Passlogix, therefore, had probable cause to commence and continue its fraud on the court allegation against Salyards because of the Hush logs, its expert's testimony concluding that no IP spoofing occurred, and remaining gaps concerning the identity of the author(s) of the anonymous e-mails. Passlogix lacked malice in commencing and continuing its claim because it acted on evidence that "seem[ed] reasonably to justify making a charge," even if Passlogix ultimately "was mistaken about the true meaning of the evidence." *Munoz*, 18 N.Y.2d at 9, 271 N.Y.S.2d 645, 218 N.E.2d 527.

For the foregoing reasons, 2FA's request to amend its counterclaims to assert a cause of action for malicious prosecution against Passlogix is denied on grounds of futility.

II. Spoliation of Evidence

Passlogix alleges that because Salyards and Cuttill admit to failing to implement a litigation hold notice and to deleting certain***409** documents during the pendency of this litigation, they should be sanctioned for spoliation of evidence. (Mem. 31.) The destroyed documents include: (1) an anonymous e-mail received by Salyards in June or July 2009 containing an attachment of Passlogix functional specifications; (2) at least 143 written communications between Salyards and Collier; and (3) 2FA network and computer logs from Cuttill's inspection of 2FA's computers and computer network. (*Id.* 31–32.) As a result of 2FA's purported spoliation of evidence, Passlogix asks for three forms of relief. First, Passlogix requests that an adverse inference be drawn that the deleted documents would have been harmful to 2FA and beneficial to Passlogix. (*Id.* 33.) Second, Passlogix requests that 2FA be precluded from making arguments implicating the discarded documents. (*Id.*) Third, Passlogix asks that Salyards be responsible for the cost of Passlogix's investigation, which was more costly and protracted as a result of Salyards' destruction of documents. (*Id.* 34.)

A. Legal Standard

[18][19][20] "Spoliation refers to the destruction or material alteration of evidence or to the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." *Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC,* 685 F.Supp.2d 456, 465 (S.D.N.Y.2010); *see also West v. Goodyear Tire & Rubber Co.,* 167 F.3d 776, 779 (2d Cir.1999); *Scalera v. Electrograph Sys.,* 262 F.R.D. 162, 170 (E.D.N.Y.2009); *Zubulake v. UBS Warburg LLC,* 229 F.R.D. 422, 430 (S.D.N.Y.2004) (" *Zubulake V* "). "The right to impose sanctions for spoliation arises from a court's inherent power to control the judicial process and litigation, but the power is limited to that necessary to redress conduct 'which abuses the judicial process.' " *Pension,* 685 F.Supp.2d at 465 (quoting *Chambers,* 501 U.S. at 45, 111 S.Ct. 2123). A party seeking sanctions for spoliation of evidence must establish:

> (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a "culpable state of mind" and (3) that the destroyed evidence was "relevant" to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense.

Zubulake V, 229 F.R.D. at 430; *see also Byrnie v. Town of Cromwell, Bd. of Educ.,* 243 F.3d 93, 107–11 (2d Cir.2001); *Scalera,* 262 F.R.D. at 170–71. The Court analyzes each of these three elements below.

1. *Duty to Preserve*

[21][22] A litigant has the "duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request." *Turner v. Hudson Transit Lines, Inc.,* 142 F.R.D. 68, 72 (S.D.N.Y.1991) (citation omitted); *see also Kronisch v. United States,* 150 F.3d 112, 126 (2d Cir.1998); *In re NTL, Inc. Sec. Litig.,* 244 F.R.D. 179, 193 (S.D.N.Y.2007). "[N]o duty to preserve arises unless the party possessing the evidence has notice of its relevance." *Turner,* 142 F.R.D. at 72–73. A party is on notice to preserve relevant documents "when litigation is reasonably anticipated," *Pension,* 685 F.Supp.2d at 461, and "at least by the time the complaint [is] served," *Turner,* 142 F.R.D. at 73. "This obligation to preserve relevant evidence exists whether or not the evidence has been specifically requested in a demand for discovery." *Scalera,* 262 F.R.D. at 171; *see also* ***410***Barsoum v. N.Y.C. Hous. Auth.,* 202 F.R.D. 396, 400 (S.D.N.Y.2001).

[23] After obtaining notice of the litigation, a party " 'must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents.' " *Pension,* 685 F.Supp.2d at 466 (quoting *Treppel v. Biovail Corp.,* 249 F.R.D. 111, 118 (S.D.N.Y.2008)); *see also Toussie v. County of Suffolk,* No. 01 Civ. 6716, 2007 WL 4565160, at *7 (E.D.N.Y. Dec. 21, 2007) ("[O]nce the duty to preserve attaches, at a minimum, a litigant is expected to 'suspend

its routine document and retention/destruction policy and to put in place a litigation hold.' ") (quoting *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y.2003) (" *Zubulake IV*")). The requirement to issue a written litigation hold notice has been in place in this District since the *Zubulake V* decision in July 2004. *See Pension*, 685 F.Supp.2d at 476–77 (stating that plaintiffs' failure to institute a litigation hold notice by 2005 when the action was transferred to the Southern District of New York was grossly negligent in light of the requirement that "was clearly established in this District by mid [-]2004"). "The preservation obligation runs first to counsel, who has 'a duty to advise his client of the type of information potentially relevant to the lawsuit and of the necessity of preventing its destruction.' " *Chan v. Triple 8 Palace, Inc.*, No. 03 Civ. 6048, 2005 WL 1925579, at *6 (S.D.N.Y. Aug. 11, 2005) (quoting *Turner*, 142 F.R.D. at 73); *see also Zubulake V*, 229 F.R.D. at 439 ("[C]ounsel has a duty to effectively communicate to her client its discovery obligations so that all relevant information is discovered, retained, and produced.... In addition, when the duty to preserve attaches, counsel must put in place a litigation hold and make that known to all relevant employees by communicating with them directly. The litigation hold instructions must be reiterated regularly and compliance must be monitored.").

[24] Once on notice of litigation, "the failure to issue a *written* litigation hold constitutes gross negligence because that failure is likely to result in the destruction of relevant information." *Pension*, 685 F.Supp.2d at 465 (emphasis in original); *see also Crown Castle USA Inc. v. Fred A. Nudd Corp.*, No. 05 Civ. 6163T, 2010 WL 1286366, at *13 (W.D.N.Y. Mar. 31, 2010) (holding plaintiff grossly negligent for failing to implement a litigation hold, which led to the destruction of documents); *Richard Green (Fine Paintings) v. McClendon*, 262 F.R.D. 284, 290 (S.D.N.Y.2009) ("[T]he failure to implement a litigation hold is, by itself, considered grossly negligent behavior."); *Toussie*, 2007 WL 4565160, at *8; *Chan*, 2005 WL 1925579, at *7 ("[T]he utter failure to establish any form of litigation hold at the outset of litigation is grossly negligent."). In one case, however, this District has found negligence, rather than gross negligence, when a party failed to institute a litigation hold but then corrected its failure. *See Pension*, 685 F.Supp.2d at 489 n. 179 (holding seven plaintiffs negligent, rather than grossly negligent, for failing to issue a litigation hold by 2005 where all plaintiffs issued such a notice by 2007 and where instituting the litigation hold in 2005 may not have made any difference because the electronic records that existed in 2003 very likely would have been lost or destroyed by 2005).

2. *Culpable State of Mind*

[25][26] In the spoliation context, a culpable state of mind includes ordinary negligence. *See Zubulake V*, 229 F.R.D. at 431; *see also* ***411***Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 108 (2d Cir.2002). "When evidence is destroyed in bad faith (i.e., intentionally or willfully), that fact alone is sufficient to demonstrate relevance." *Zubulake V*, 229 F.R.D. at 431; *see also Residential Funding*, 306 F.3d at 108–09. By contrast, when the destruction is negligent, grossly negligent, or reckless, relevance must be proven by the party seeking sanctions. *See Zubulake IV*, 220 F.R.D. at 221 ("[B]ecause UBS's spoliation was negligent and possibly reckless, but not willful, [plaintiff] must demonstrate that a reasonable trier of fact could find that the missing e-mails would support her claims."); *see also Richard Green*, 262 F.R.D. at 291.

[27] "No matter what level of culpability is found, ... the spoliating party should have the opportunity to demonstrate that the innocent party has not been prejudiced by the absence of the missing information." *Pension*, 685 F.Supp.2d at 468. To show prejudice, "[t]he moving party usually sets forth some type of extrinsic evidence as to the content of missing materials which demonstrates the extent to which such materials would have been harmful to the spoliator." *Skeete v. McKinsey & Co., Inc.*, No. 91 Civ. 8093, 1993 WL 256659, at *7 (S.D.N.Y. July 7, 1993) (Leisure, J.). "If the spoliating party offers proof that there has been no prejudice, the innocent party, of course, may offer evidence to counter that proof." *Pension*, 685 F.Supp.2d at 468.

3. *Relevance*

[28][29] In the spoliation context, relevance "means something more than sufficiently probative to satisfy Rule 401 of the Federal Rules of Evidence." *Chan,* 2005 WL 1925579, at *7; *see also Residential Funding,* 306 F.3d at 108–09. A discarded document is relevant where a reasonable trier of fact could find that the document either would harm the spoliator's case or support the innocent party's case. *See Port Auth. Police Asian Jade Soc'y of N.Y. & N.J. Inc. v. Port Auth. of N.Y. & N.J.,* 601 F.Supp.2d 566, 570 (S.D.N.Y.2009) (" '[R]elevant' means that the evidence must be of the sort that a reasonable jury could find harmful to the spoliator's case."); *Zubulake V,* 229 F.R.D. at 430 (stating that a discarded document is "relevant" to the victimized party's "claim or defense" where "a reasonable trier of fact could find that [the missing document] would support that claim or defense"). "[R]elevance 'may be inferred if the spoliator is shown to have a sufficiently culpable state of mind.' " *Scalera,* 262 F.R.D. at 178 (quoting *Chan,* 2005 WL 1925579, at *8). To have a sufficiently culpable state of mind warranting a relevance inference, the spoliator must have acted in bad faith—that is, intentionally or willfully. *See In re Methyl Tertiary Butyl Ether Prods. Liab. Litig.,* 643 F.Supp.2d 482, 496 (S.D.N.Y.2009); *Zubulake V,* 229 F.R.D. at 431; *Zubulake IV,* 220 F.R.D. at 221; *Turner,* 142 F.R.D. at 77. "Although many courts in this district presume relevance where there is a finding of gross negligence, application of the presumption is not required." *Pension,* 685 F.Supp.2d at 467; *see also Residential Funding,* 306 F.3d at 109 ("[A] showing of gross negligence in the destruction or untimely production of evidence will in some circumstances suffice, standing alone, to support a finding that the evidence was unfavorable to the grossly negligent party."); *Treppel,* 249 F.R.D. at 121–22 ("While it is true that under certain circumstances 'a showing of gross negligence in the destruction or untimely production of evidence' will support [a relevance] inference, the circumstances here do not warrant such a finding, as the defendants' conduct 'does not rise to the egregious level seen in cases where relevance is determined as a matter of law.' " (quoting ***412** *Residential Funding,* 306 F.3d at 109 and *Toussie,* 2007 WL 4565160, at *8)).

[30] In the absence of bad faith destruction of evidence, "the moving party may submit extrinsic evidence tending to demonstrate that the missing evidence would have been favorable to it." *Chan,* 2005 WL 1925579, at *8. Moreover, "when the spoliating party [is] merely negligent, the innocent party must prove both relevance and prejudice in order to justify the imposition of a severe sanction." *Pension,* 685 F.Supp.2d at 467–68; *see also Byrnie,* 243 F.3d at 108 ("[T]he burden falls on the 'prejudiced party' to produce 'some evidence suggesting that a document or documents relevant to substantiating [its] claim would have been included among the destroyed files.' " (quoting *Kronisch,* 150 F.3d at 128)). The innocent party may do so by presenting " 'extrinsic evidence tending to show that the destroyed e-mails would have been favorable to [its] case.' " *Pension,* 685 F.Supp.2d at 468 (quoting *Toussie,* 2007 WL 4565160, at *8).

B. Application

[31] To establish that Salyards engaged in spoliation of evidence by deleting the documents at issue, Passlogix must show by a preponderance of the evidence that, for each category of documents: (a) Salyards had a duty to preserve the documents at the time they were destroyed; (b) Salyards destroyed the documents with a culpable state of mind; and (c) the destroyed documents were relevant to Passlogix's claim or defense. *See Pension,* 685 F.Supp.2d at 467–68; *Zubulake V,* 229 F.R.D. at 430; *Scalera,* 262 F.R.D. at 170–71. For the reasons set forth below, the Court holds that although Passlogix has satisfied the first two elements—duty and culpable state of mind—with respect to all three categories of deleted documents, it has satisfied the final relevance prong only with respect to the latter two: (2) written communications between Salyards and Collier, and (3) logs from Cuttill's investigation of 2FA's computers and computer network. As a sanction for 2FA's spoliation of documents, the Court orders 2FA to pay a fine of $10,000.

1. *June/July Anonymous E-mail*

Salyards testified at his deposition and at the evidentiary hearing that he received an anonymous e-mail around

late June or early July 2009 that included an attachment containing Passlogix functional specifications (the "June/July e-mail"). (Tr. 356:7–22, 357:11–17.) Salyards could not recall the e-mail address from which the June/July e-mail was sent, except that he believed it came from a "hushmail.com" domain name. (Tr. 357:2–10.) After receiving the June/July e-mail, which was sent only to him, Salyards testified that he spent about forty-five minutes to an hour reading the attachment, then showed it to Cuttill. (Tr. 356:10–11, 358:13–19.) After reading and discussing the document, both Salyards and Cuttill decided it was improper for them to have it, so Salyards deleted it without disclosing it to his attorney or Passlogix. (Tr. 358:18–359:2.) Salyards notes that this attachment was similar to one of the attachments to the September 3 e-mail. (Tr. 436:14–437:2.)

Passlogix first contends that Salyards is lying about the existence of the June/July e-mail "to cover up his role in the other two emails." (PX 33 at 4 n. 1.) Passlogix asserts that Salyards' claim that he deleted the attachment to the June/July e-mail is not credible when juxtaposed with Salyards' push "for expansive discovery based on his review of the computer specifications attached to the September 3 E-mail," which, according to Salyards, contained similar content. (Reply Mem. 13.) The Court, however, finds Salyards' testimony ***413** about the existence of the June/July e-mail credible because he first testified about the e-mail at a deposition that took place before Passlogix brought its fraud on the court claim, thereby refuting Passlogix's argument that Salyards had a motive to lie about the June/July e-mail to cover-up his role in the other two e-mails. (PX 33 at 4 n. 1.)

Alternatively, Passlogix argues that, assuming that the June/July e-mail existed, Salyards engaged in spoliation of evidence by deleting it. Salyards concedes that he deleted the June/July e-mail. (Tr. 357:18–358:5.) 2FA contends that Salyards' deletion of the June/July e-mail is not spoliation because the e-mail "was not evidence when Mr. Salyards deleted it" and "[t]he attachment was a Passlogix document, which is still in its possession." (Opp'n Mem. 29.) Moreover, 2FA asserts that even if the June/July e-mail "were evidence, it would only help show the misappropriation of intellectual property and is favorable to 2FA." (*Id.*) 2FA also contends that Salyards' deletion of the June/July e-mail was no different from Boroditsky's, Passlogix's CEO's, request that the recipients of the September 3 e-mail delete that e-mail and its attachments. (*Id.* 29–30; Tr. 89:15–21.)

a. *Duty*

[32] The Court holds that 2FA had a duty to preserve the June/July e-mail at the time that Salyards deleted it. According to Salyards, the June/July e-mail contained Passlogix technical specifications that he and Cuttill recognized they should not possess. (Tr. 358:13–359:2.) 2FA states that Salyards' deletion of the June/July e-mail was not spoliation because "[t]he attachment was a Passlogix document, which is still in [Passlogix's] possession." (Opp'n Mem. 29). The significance of the June/July e-mail, however, is not that Passlogix may have a copy of the proprietary attachment, but that the attachment was *sent* to Salyards. (Tr. 356:10–11.)

"While a litigant is under no duty to keep or retain every document in its possession once a complaint is filed," the June/July e-mail is particularly germane to the underlying litigation which involves a claim by 2FA that Passlogix misappropriated its intellectual property. *Turner*, 142 F.R.D. at 72. Although 2FA argues that the June/July e-mail was not evidence when Salyards deleted it, 2FA's duty to preserve extends not only to evidence, but to what "is reasonably calculated to lead to the discovery of admissible evidence" or is "reasonably likely to be requested during discovery." *Id.* (citation and internal quotation marks omitted); *see also Arista Records LLC v. Usenet.com, Inc.*, 608 F.Supp.2d 409, 433 (S.D.N.Y.2009). An e-mail transmitting Passlogix's own propriety information, even if not evidence itself, may lead to the discovery of admissible evidence regarding Passlogix's intellectual property safeguarding practices. *See Arista*, 608 F.Supp.2d at 433; *Turner*, 142 F.R.D. at 72. Because 2FA's duty to preserve documents related to Passlogix's underlying lawsuit attached, at minimum, on December 18, 2008, when Passlogix filed its original complaint, Salyards was

on notice of the June/July e-mail's relevance when he deleted it shortly after receiving it in June or July 2009. *See Turner*, 142 F.R.D. at 73.

For the foregoing reasons, the Court holds that Salyards violated his duty to preserve documents when he deleted the June/July e-mail.

b. *Culpable State of Mind*

The Court holds that Salyards was grossly negligent in deleting the June/July e-mail. Notwithstanding his obligation to preserve documents, Salyards testified that 2FA never implemented a litigation ***414** hold and continues to delete e-mails routinely. (Tr. 353:9–14, 449:23–450:7, 451:11–14; PX 43 ¶ 2.) Passlogix contends that 2FA's failure to implement a litigation hold/document retention notice, standing alone, warrants sanctions. (Mem. 31; Reply Mem. 12.)

[33] As detailed above, "the failure to implement a litigation hold is, by itself, considered grossly negligent behavior." *Richard Green*, 262 F.R.D. at 290. Because Salyards admits that 2FA did not, and does not, have a litigation hold/document preservation policy, Passlogix "has clearly satisfied its burden with respect to the second prong of the spoliation test." *Id.* at 291. Thus, the Court holds that 2FA acted with gross negligence by deleting the June/July e-mail in the absence of a litigation hold during the pendency of this litigation.

c. *Relevance*

Because there is insufficient evidence indicating that Salyards deleted the June/July e-mail in bad faith, the Court does not infer relevance. Likewise, the Court declines to infer relevance based on 2FA's grossly negligent failure to institute a litigation hold because 2FA's conduct, in the context of its overall document production in this case, "does not rise to [an] egregious level." *Toussie*, 2007 WL 4565160, at *8. Therefore, to satisfy the relevance requirement, Passlogix must submit extrinsic evidence tending to demonstrate that the missing evidence would have been favorable to it. *See Chan*, 2005 WL 1925579, at *8.

Although "the burden placed on the moving party to show that the lost evidence would have been favorable to it ought not be too onerous," *id.* at *7, Passlogix submits no extrinsic evidence tending to show that the June/July e-mail would have been favorable to it. Passlogix states that had the June/July e-mail been preserved, the parties may have been able to track down the IP address and other information identifying the sender and, thereby, test the bonafides of Salyards' IP address spoofing defense. (Mem. 34.) However, the only way the June/July e-mail could be relevant to Passlogix, i.e., support its theory that Salyards is the author of the anonymous Hush emails, is if—implausibly—Salyards sent the June/July e-mail to himself. If, on the other hand, the June/July e-mail indicated that someone other than Salyards was the author, then the e-mail would harm, rather than support, Passlogix's theory that Salyards is the author of these anonymous Hush e-mails. Since Passlogix cannot point to extrinsic evidence tending to show that Salyards authored the June/July e-mail, the Court is "not persuaded on this record that a reasonable [trier of fact] could find that the [June/July e-mail] was harmful" to 2FA or helpful to Passlogix. *Adorno v. Port Auth. of N.Y. & N.J.*, 258 F.R.D. 217, 229 (S.D.N.Y.2009) (Chin, J.); *see also Port Auth. Police Asian Jade Soc'y*, 601 F.Supp.2d at 570 (denying motion for sanctions for spoliation where moving party could not demonstrate that evidence would have been unfavorable to the spoliator); *Hamre v. Mizra*, No. 02 Civ. 9088, 2005 WL 1083978, at *3 (S.D.N.Y. May 9, 2005) (Leisure, J.) (denying plaintiffs' request for adverse inference where they "did not put forth *any* evidence" indicating that destroyed documents would corroborate their theory of the case (emphasis in original)). To the extent that Passlogix's investigation into Hush-related e-mail activity was more burdensome and expensive as a result of Salyards' deletion of the June/July e-mail, (Mem. 34), the court discerns no prejudice to Passlogix going to the merits of the ***415** case, and Passlogix points to none. *See Pension*, 685 F.Supp.2d at 467–68.

For the foregoing reasons, the Court holds that al-

though 2FA had a duty to preserve the June/July e-mail and was grossly negligent in deleting it, it did not engage in spoliation of evidence because Passlogix has failed to establish that the email would have been helpful to its claims or defenses or harmful to 2FA's claims or defenses.

2. *Written Communications between Collier and Salyards*

[34] Passlogix contends that Salyards engaged in the spoliation of evidence by deleting at least 143 written communications with Collier during the pendency of this litigation. (Mem. 31–32.) These destroyed documents consist of at least twelve e-mails, ninety-one text messages, and forty Skype messages.[FN10] (*Id.* 31.) Passlogix states that because Collier used his personal, rather than his work, computer to engage in most of these communications, there was no way for Passlogix to obtain a copy of most of these records. (Reply Mem. 13 n. 13.) 2FA acknowledges that it did not preserve these written communications, but states that Collier's involvement in this litigation "was only known to 2FA in late November 2009" and that "neither Mr. Salyards nor 2FA had any knowledge, or reason to know, that any documents related to Chris Collier might be relevant in this case, which anyway they are not." (Opp'n Mem. 30.) 2FA also points out that Passlogix has obtained some of the e-mails, phone records, and Skype messages, resulting in no prejudice to Passlogix. (*Id.*)

> FN10. Skype is an internet software application that, among other features, allows users to engage in instant messaging.

To address the discarded the written communications between himself and Collier during the pendency of this litigation, Salyards submits an affidavit outlining their correspondence based on a review of his phone records, travel calendar, and discussions with Cuttill. (PX 43 ¶ 5.) Salyards recalls corresponding with Collier via e-mail "approximately 12 times in 2009" and that "eight of the exchanges were during [Collier's] tenure at Passlogix," which was from April 1, 2009 to November 16, 2009. (*Id.*) Salyards states that these e-mails generally concern possible business opportunities and consist of statements such as, "let's talk about something. Phone call, let's talk about a lot." (*Id.* ¶ 3; *see also* Tr. 440:10–13.) With respect to the content of the unsaved text messages, Salyards states that "they were routinely confirming the ability or inability to answer a call, the arrival at a restaurant at a specific time or our respective locations on the lake," and consisted of phrases such as "I'm leaving, lunch, I'm here, be five minutes." (PX 43 ¶ 13; *see also* Tr. 440:4–9.)

The Skype records that Passlogix obtained from Collier's work computer indicate that the Skype messages between Salyards and Collier mainly concern lunch plans or social activities. (*See* PX 50; Tr. 46:1–7, 124:20–127:5.) These Skype records corroborate Salyards' description of the typical Skype exchanges between him and Collier. (*See* Tr. 442:25–443:10 (Salyards testifying that the typical Skype messages between him and Collier consisted of statements like "you busy," "on the phone," "cool," and "where").) Passlogix, however, claims that some of the Skype communications concern topics at issue in the underlying litigation and, therefore, should have been preserved. (Reply Mem. 13.)

***416** Passlogix also points to Collier's secret visits with Salyards at 2FA's office as circumstantial proof that their interactions related to the underlying litigation. Salyards acknowledges that from April 2009 through November 16, 2009, Collier came to 2FA's office at least seven times, but that Salyards "was always under the impression that [Collier] had full endorsement from Passlogix and was acting as a go between" for Passlogix's interest in a software product that 2FA had licensed to HID Global, 2FA's largest customer who also maintains a business relationship with Passlogix. (PX 43 ¶¶ 6 & 5(f)(a).)

a. *Duty*

Salyards admits that he did not preserve the 143 written communications he had with Collier. (Tr. 354:21–355:25.) Salyards testified that 2FA does not have a document retention policy, that he routinely deletes e-mails and text messages, and that his Skype logs are retained for about two weeks and then are purged automatically. (Tr. 449:23–451:4; PX 43 ¶ 2.)

As already discussed, by December 18, 2008, Salyards had a duty to preserve documents related to the underlying litigation. That duty extends to documents concerning, but not limited to, the misappropriation of intellectual property and the parties' obligations and performance under their licensing agreement. (*See generally* Compl.; Am. Compl.; Answer & Countercl.) The issue is whether Salyards was on notice that some of his written communications with Collier were probative of the underlying litigation when the communications were deleted. The Court holds that he was.

Salyards' affidavit accounts for at least one e-mail from mid-August 2009, in which Collier asks for Salyards' "help coordinating the development effort with HID" to "get naviGO into [Passlogix's] authenticator program." (PX 43 57 5(g).) NaviGo is a 2FA software product that 2FA licensed to HID Global, 2FA's largest customer, who also maintains a business relationship with Passlogix. (*Id.* ¶ 5(f)(a).) Salyards states that he referred Collier to two other 2FA employees for assistance, and that he and Collier "had several follow-up conversations on this topic." (*Id.* ¶ 5(g).) Such an e-mail, which discusses a potential business opportunity between Passlogix and 2FA, is probative of the parties' underlying dispute, which arises from Passlogix's prior licensing of 2FA's software. Passlogix also contends that a Skype message from April 30, 2009, in which Salyards asks Collier, "do you have access to PLX Admini-track?" (PX 50 at PL961801), implicates "the very subject of discovery disputes before the Magistrate Judge" and constitutes communication "about product bugs and maintenance matters at issue in the case." (Reply Mem. 13.) Salyards acknowledges that he "talk[ed] to [Collier] about PLX AdminiTrack," which is a "detrack or bug defect tracking system," around the same timeframe that 2FA sent Passlogix a discovery request for "all historical and present AdminiTrack items ever entered." (Tr. 460:17–462:17; PX 63 ¶ 27.) This Skype message relates to a discovery request regarding software maintenance matters at issue in the underlying litigation and, therefore, should have been preserved.

For the reasons above, Salyards had a duty to preserve written communications with Collier pertaining to, at a minimum, 2FA's software and business opportunities with Passlogix as well as maintenance matters related to software at issue in the parties' underlying lawsuit. By failing to preserve such documents, including the aforementioned e-mail and Skype message, Salyards breached his duty to preserve documents.

***417** b. *Culpable State of Mind*

[35] 2FA argues that neither Salyards nor 2FA acted willfully or negligently in deleting the communications with Collier, who was not involved in this case until late November 2009. (Opp'n Mem. 32.) As already discussed, even if Collier was not involved actively in the instant fraud on the court dispute until late November 2009, at least two of Salyards' written communications with Collier relate to issues involved in the underlying litigation. Salyards' failure to preserve these written communications, in addition to 2FA's overall failure to issue a litigation hold notice, constitutes gross negligence.

c. *Relevance*

Passlogix provides extrinsic evidence that the written communications that Salyards discarded would support Passlogix's position in the underlying litigation. The April 30, 2009 Skype message, in which Salyards suggests that Collier report a software problem on Passlogix's Admini-Track system, directly relates to a discovery request in the underlying litigation. However, because Passlogix obtained a copy of these Skype communications from Collier's work computer, it is not prejudiced by their deletion. *See Pension,* 685 F.Supp.2d at 468 ("[T]he spoliating party should have the opportunity to demonstrate that the innocent party has not been prejudiced by the absence of the missing information."); *Ispat Inland, Inc. v. Kemper Envtl., Ltd.*, No. 05 Civ. 5401, 2006 WL 3478339, at *3 (S.D.N.Y. Nov. 30, 2006) (denying defendant's motion for sanctions for alleged perjury and spoliation of evidence where, although deponent, in-house counsel at plaintiff corporation, admitted to discarding documents used to refresh his recollection prior to his deposition, defendant's counsel had duplicates in his actual possession at the de-

position).

[36] The record provides additional extrinsic evidence that the deleted communications between Salyards and Collier were relevant. The e-mail that Salyards deleted in mid-August 2009, in which Salyards sought to help Collier "get naviGO into [Passlogix's] authenticator program," (PX 43 ¶ 5(g)), provides extrinsic proof that this communication, if preserved, could support Passlogix's defense to 2FA's misappropriation of intellectual property claim. This communication could lead a reasonable factfinder to cast doubt on 2FA's misappropriation claim where 2FA, a purported victim of Passlogix's misappropriation of its intellectual property, pursues a business opportunity with Passlogix involving 2FA's intellectual property in the midst of a lawsuit relating to the fall-out of a prior such relationship. Because Passlogix does not have a copy of this e-mail and because Salyards' description of the e-mail in his affidavit does not supplant the missing document, Passlogix is prejudiced by its deletion.

For the reasons stated above, the Court holds that, in failing to preserve written communications between Salyards and Collier concerning software maintenance matters and potential business opportunities between 2FA and Passlogix, 2FA engaged in the spoliation of evidence.

3. *2FA's Computer and Network Logs from Cuttill's Investigation*

Passlogix alleges that 2FA failed to preserve evidence from Cuttill's personal inspection of 2FA's computers and computer network. (Mem. 32.) 2FA responds that Passlogix was aware of Cuttill's inspection since December 1, 2009, when Cuttill testified about it during his deposition, "but never requested anything from 2FA in this regard, and never made any requests in the several appearances before Judge Dolinger." (Opp'n 32.) Passlogix responds that, during Cuttill's deposition, 2FA's ***418** counsel blocked questioning pertaining to Cuttill's investigation, citing attorney client and work product privileges, yet later admitted that counsel was not involved in the investigation. (Mem. 32; Tr. 571:11–20; 12/22/09 J. Dolinger Hr'g Tr. 24:24–28:4.)

At the evidentiary hearing, Cuttill testified that in late October or early November 2009, he interviewed people who had access to 2FA's network on September 3 and checked all of 2FA's computers for evidence of the attachments to the September 3 e-mail and found no evidence that anyone at 2FA sent that e-mail. (Tr. 572:25–575:5.) He also testified that he interviewed people that he thought had access to 2FA's network in April but did not interview Collier since the interviews were conducted before Collier's confession. (Tr. 573:6–14.) Cuttill did not take notes during his interviews and investigation. (Tr. 573:15–16.) Cuttill also said that he reviewed 2FA's computer logs but did not produce those logs because they were "indiscernible" and "inconclusive." (Tr. 575:6–578:21.) Cuttill explains that the September logs "were tainted" because, by the time he conducted his investigation, "the most recent cookies were all from ... the second or third week of September" and "[t]here was nothing from September 3rd." (Tr. 577:1–7.) Cuttill testified that during the second or third week of September, he and Salyards had visited Hush "to find out what Hushmail was all about." (Tr. 577:3–16.) Therefore, had these logs been produced, Passlogix "would have come back and said, 'But if he accessed it [in mid-September], what if he accessed it before?' And that wouldn't have been proof of anything." (Tr. 577:11–16.) Then Cuttill said that "[t]here were some security logs that show that Greg Salyards' computer was locked" on September 3, but 2FA did not produce those logs either—even though they appear helpful to 2FA's position—because "[t]hey weren't asked for, and to be honest, we were moving so quickly in this that I–I don't know." (Tr. 578:10–18.) Cuttill offered to produce these logs with 2FA's post-hearing brief, though the Court has no record of any logs from Cuttill's investigation ever being produced. (Tr. 578:15–19.)

a. *Duty*

Cuttill admits that his investigation took place after Passlogix sent its letter to the Court accusing Salyards of authoring the anonymous e-mails and, therefore, after 2FA's duty to preserve documents related to the authorship of the April 13 and September 3 e-mails attached. (Tr.

573:10–13.) Even if Passlogix had not requested the logs, as 2FA contends, the duty to preserve documents is not limited solely to documents that are "the subject of a pending discovery request"; rather, the duty extends to documents "reasonably likely to be requested during discovery." *Turner,* 142 F.R.D. at 72. Since Cuttill affirmatively undertook his investigation, he had a duty to preserve the fruits of that investigation, whether ripe or rotten. Because 2FA requested information from Passlogix's internal investigation, it was reasonable for 2FA to expect that Passlogix, likewise, would request documents related to any investigation 2FA conducted. Even if 2FA no longer had its April 2009 and September 3 computer logs by the time Cuttill conducted his investigation, Cuttill had a duty to preserve the logs that *were* available-that is, the mid-September logs, which Cuttill admits were accessible. *See Treppel,* 249 F.R.D. at 119 ("[I]t is ... clear that [defendant] should have retained the monthly backup tapes of the relevant servers from the previous year, since these were quite likely to contain files that were later deleted"); *Zubulake IV,* 220 F.R.D. at 218 ("If a company can identify where particular employee documents are stored on backup tapes, then the tapes ... should ***419** be preserved if the information contained on those tapes is not otherwise available."). 2FA, therefore, breached its duty to preserve documents when it did not retain the computer logs that Cuttill reviewed.

b. *Culpable State of Mind*

As already discussed, 2FA never implemented a litigation hold notice at any point in this litigation. At minimum, therefore, Cuttill acted with gross negligence by failing to preserve the computer logs from his late October/early November 2009 investigation. Moreover, Cuttill admitted that he intentionally withheld the logs because of his subjective belief that the logs would have appeared to point falsely to Salyards as the author of the September 3 e-mail. The duty to preserve documents is meant to prevent these sorts of "judgment calls" by litigants and, instead, requires parties to preserve all documents that may reasonably lead to the discovery of relevant evidence, regardless of whether those documents appear to create false positives or false negatives. *See Pension,* 685 F.Supp.2d at 473 (disparaging document preservation policy that "place[d] total reliance on the employee to search and select what that employee believed to be responsive records"). Thus, 2FA acted in bad faith by failing to preserve records that it thought falsely pointed to Salyards as the author of the September 3 e-mail. The Court holds, therefore, that 2FA's failure to preserve the computer logs from Cuttill's investigation amounts to intentional bad faith spoliation of evidence.

c. *Relevance*

Because the Court finds that Cuttill intentionally and in bad faith failed to preserve 2FA's computer logs from his investigation, the Court presumes the relevance of these documents, obviating Passlogix's burden to show through extrinsic evidence that these documents would have been favorable to its position. *See Pension,* 685 F.Supp.2d at 467–68. The burden now shifts to 2FA to demonstrate that Passlogix was not "prejudiced by the absence of the missing information." *Id.* at 468FA states that Passlogix knew about Cuttill's investigation "on December 1st but never requested anything from 2FA ... and never made any requests in the several appearances before Judge Dolinger." (Opp'n Mem. 32–33.) This representation clearly misrepresents the record. During a December 22 hearing before Judge Dolinger, which occurred after Cuttill's deposition, Passlogix explicitly requested, and Judge Dolinger ordered 2FA to produce, information from Cuttill's investigation. (*See* 12/22/09 J. Dolinger Hr'g Tr. 24:24–28:4 (Passlogix's counsel requesting "any notes, findings, documentation surrounding the 2FA internal investigation within the 2FA company concerning the anonymous e-mails" and Judge Dolinger ordering 2FA's counsel to "inquire of [his] client and advise counsel for Passlogix within ... three days" about 2FA's internal investigation).). There is no dispute that the records that 2FA provided to Passlogix did not include the electronic records from Cuttill's investigation. In defense of its actions, 2FA contends that it agreed to allow Passlogix to conduct forensic examinations on all of 2FA's computers, but Passlogix never did so. (Opp'n Mem. 32–33.) 2FA's argument misses the point. Making its computers available to Passlogix for inspection does not absolve 2FA of its affirma-

tive duty to preserve electronic records that it examined but admittedly failed to preserve. Because 2FA failed to preserve the electronic records, making its computers available for inspection likely would have been a meaningless gesture.

Moreover, 2FA's position that Passlogix never asked for the computer logs—even if true—is disingenuous in light of 2FA preventing Passlogix, on seemingly erroneous ***420** privilege grounds, from asking Cuttill during his deposition about the scope of his investigation. (Mem. 4; Tr. 596:22–598:20; 12/22/09 J. Dolinger Hr'g Tr. 24:24–28:4.) 2FA's counsel and Cuttill later admitted that counsel was not involved in Cuttill's investigation. (*See* Tr. 596:22–597:25; 12/22/09 J. Dolinger Hr'g Tr. 25:10–26:17.) Though considered, the Court declines to issue a separate sanction for 2FA's possibly erroneous assertion of privilege, as the Court deems 2FA's sanction for spoliation of evidence sufficient to prevent future litigation misconduct.

Because Passlogix does not have a copy of 2FA's computer logs and because the logs likely are no longer available as a result of 2FA's continued deletion of records, the Court holds that Passlogix is prejudiced by 2FA's spoliation of these electronic records.

C. Remedy for 2FA's Spoliation of Evidence

[37][38][39][40] "The court has the inherent power to impose sanctions for the spoliation of evidence, even where there has been no explicit order requiring the production of the missing evidence." *Scalera*, 262 F.R.D. at 171; *see also Residential Funding*, 306 F.3d at 106–07. "The determination of an appropriate sanction for spoliation, if any, is confined to the sound discretion of the trial judge and is assessed on a case-by-case basis." *Fujitsu Ltd. v. Fed. Express Corp.*, 247 F.3d 423, 436 (2d Cir.2001); *see also Reilly v. Natwest Mkts. Group Inc.*, 181 F.3d 253, 267 (2d Cir.1999) ("Trial judges should have the leeway to tailor sanctions to insure that spoliators do not benefit from their wrongdoing—a remedial purpose that is best adjusted according to the facts and evidentiary posture of each case."). Sanctions for the spoliation of evidence are meant to (1) deter parties from destroying evidence; (2) place the risk of an erroneous evaluation of the content of the destroyed evidence on the party responsible for its destruction; and (3) restore the party harmed by the loss of evidence helpful to its case to where the party would have been in the absence of spoliation. *See Potenza v. Gonzales*, Nos. 5:07–CV–225, 5:07–CV226, 2010 WL 890959, at *3 (N.D.N.Y. Mar. 8, 2010); *Byrnie*, 243 F.3d at 107; *Port Auth. Police Asian Jade Soc'y*, 601 F.Supp.2d at 570. "[A] court should always impose the least harsh sanction that can provide an adequate remedy." *Pension*, 685 F.Supp.2d at 469. "The choices include—from least harsh to most harsh—further discovery, cost-shifting, fines, special jury instructions, preclusion, and the entry of default judgment or dismissal (terminating sanctions)." *Id.*

Passlogix asks for three forms of relief for 2FA's spoliation of evidence—an adverse inference, preclusion, and costs. (Mem. 33–34.) The Court declines to impose any of these sanctions, concluding that the most appropriate sanction for 2FA's spoliation of evidence is a monetary fine.

1. *Adverse Inference*

[41] An adverse inference is warranted where a party intentionally destroys documents that it is obligated to preserve and that are relevant to its adversary's case. *See Byrnie*, 243 F.3d at 107–08; *Kronisch*, 150 F.3d at 126. Passlogix asks the Court to infer from the deleted communications between Salyards and Collier that Salyards and Collier conspired to send the anonymous e-mails and to have Collier falsely testify to authoring the April 13 e-mail. In support of its adverse inference request, Passlogix points to phone records and Skype logs indicating that Collier and Salyards communicated during critical points in the litigation: (1) April 13 when the first anonymous e-mail was sent; (2) ***421** September 4, 2009, the day after the next anonymous e-mail was sent; and (3) between October 26–28, when Salyards learned that Passlogix was going to, and then did, inform that Court that Salyards authored the anonymous e-mails. (PX 43 Ex. A; PX 45 at CC10 line 212, CC100 line 68, CC124 lines 365–66, 370–71, 383, CC128 line 191, CC136 line 2; PX

47 at 11690, 11796, 11800, 11857, 11862; PX 50 at PL9618016.) Upon a review of the entire record of communications between Salyards and Collier—including their cell phone records from April through November 2009 and Skype logs from April through October 2009 that Passlogix retrieved from Collier's work computer—Salyards' and Collier's level of communication during critical points in the litigation is consistent with their level of contact throughout the course of the year. Therefore, this extrinsic evidence is inconclusive at best and does not warrant an adverse inference that the two were conspiring to commit a fraud on the court. *See Skeete,* 1993 WL 256659, at *7 (denying defendant's request for adverse inference "where defendants have not demonstrated a nexus between the content of the materials and the inference the defendants wish to have drawn").

The Court also declines to infer that the 2FA computer network logs that Cuttill failed to preserve would have shown that Salyards authored the September 3 e-mail. Through his testimony at the evidentiary hearing, Cuttill admitted that the 2FA network logs, if preserved, would have indicated that Salyards visited Hush in mid-September. The Court credits this testimony and finds that a further adverse inference is not warranted. *See Wechsler v. Hunt Health Sys., Ltd.,* 381 F.Supp.2d 135, 148–49 (S.D.N.Y.2003) (Leisure, J.) (denying request for a negative inference where, among other things, the absent documents did not have a profound effect on defendant's case).

2. *Evidence Preclusion*

[42] "Preclusion is a harsh sanction preserved for exceptional cases where a ... party's failure to provide the requested discovery results in prejudice to the requesting party." *Tracy ex rel. v. NVR, Inc.,* No. 04 Civ. 6541L, 2009 WL 3153150, at *8 n. 15 (W.D.N.Y. Sept. 30, 2009) (citation and internal quotation marks omitted); *see also Update Art, Inc. v. Modiin Publ'g, Ltd.,* 843 F.2d 67, 71 (2d Cir.1988). Passlogix asks that 2FA be precluded from arguing that Collier somehow traced Salyards' whereabouts through Salyards' e-mail headers and somehow spoofed Salyards' IP address as it changed from office, to home, to the Mark Hopkins Hotel. (Mem. 33.) The Court declines Passlogix's preclusion request as too harsh and unwarranted by the evidence in the record, as it would prohibit 2FA from asserting its IP spoofing defense. *See Pesce v. Gen. Motors Corp.,* 939 F.Supp. 160, 165 (N.D.N.Y.1996) (declining "the drastic sanction of preclusion" where "an order precluding any testimony or evidence of the [product] being defective would necessarily preclude plaintiff from being able to present a *prima facie* case," "which would be tantamount to dismissal of the action"); *see also In re WRT Energy Sec. Litig.,* 246 F.R.D. 185, 200 (S.D.N.Y.2007) (crafting a more narrow remedy where defendants' proposed sanction of precluding plaintiffs from relying on the destroyed documents "in any respect" would "sweep too broadly").

3. *Costs*

Passlogix requests that 2FA pay for its investigation, which was more costly and protracted as a result of 2FA's spoliation of evidence. (Mem. 34.) "[C]ompensable costs may arise either from the discovery ***422** necessary to identify alternative sources of information, or from the investigation and litigation of the document destruction itself." *Turner,* 142 F.R.D. at 78 (holding that "an award of costs, including attorneys' fees, is entirely warranted" where defendant "unjustifiably destroyed documents after litigation had been commenced, causing the plaintiff to expend time and effort in attempting to track down the relevant information"); *see also Pension,* 685 F.Supp.2d at 497–98 (sanctioning plaintiffs who were negligent in providing discovery by issuing a monetary sanction of reasonable costs, including attorneys' fees, associated with reviewing declarations submitted, deposing these declarants, and bringing this motion for sanctions).

[43] After careful consideration, the Court holds that costs are not appropriate here where the extra expense incurred by Passlogix—that is related solely to the deletion of electronic data from Cuttill's investigation and certain communications between Salyards and Collier—cannot be carved out easily from Passlogix's overall costs in litigating the instant dispute. Therefore, a more narrowly tailored sanction that serves to punish 2FA for its grossly negligent

failure to institute a litigation hold, intentional failure to preserve electronic records from its investigation, and possibly erroneous assertion of privilege, is more appropriate here.

4. *Monetary Fine*

[44][45] The applicable sanction for spoliation of evidence "should be molded to serve the prophylactic, punitive, and remedial rationales underlying the spoliation doctrine." *West,* 167 F.3d at 779; *see also In re Terrorist Bombings of U.S. Embassies in E. Africa,* 552 F.3d 93, 148–49 (2d Cir.2008). Imposing a fine is consistent with the Court's inherent power to sanction parties for the spoliation of evidence. *See Pension,* 685 F.Supp.2d at 469–70 (considering a fine one of the less harsh remedies a Court may choose from to sanction a party for spoliation of evidence); *accord Travelers Property Cas. of Am. ex rel. Goldman v. Pavilion Dry Cleaners,* No. Civ. A. 04–1446, 2005 WL 1366530, at *4 (D.N.J. June 7, 2005)(stating that a monetary fine may be appropriate to punish an offending party for spoliation of evidence).

[46] The Court holds that a monetary fine of $10,000 against 2FA best suits "the facts and evidentiary posture of [this] case." *Reilly,* 181 F.3d at 267. 2FA is a small company founded only in 2006, and Salyards and Cuttill—who the Court both finds responsible for the spoliation of evidence in this case—are 2FA's sole principals and co-founders. Here, a fine against 2FA serves the dual purposes of deterrence and punishment. *See Green,* 262 F.R.D. at 292. Because Salyards and Cuttill are the sole principals of 2FA, a fine directed at 2FA will affect them directly. In concluding that a fine of $10,000 is the most appropriate sanction, the Court balances 2FA's litigation conduct with its status as a small corporation. *See Shangold v. Walt Disney Co.,* 275 Fed.Appx. 72, 74 (2d Cir.2008) (stating that district courts "should not hesitate to take the relative wealth of the parties into account" when setting monetary sanctions, and affirming district court's $10,000 fee award) (citation and internal quotation marks omitted); *McMunn,* 191 F.Supp.2d. at 448, 462 (considering defendant's ability to collect from plaintiff in issuing order requiring plaintiff to pay defendant $20,000 with interest for, among other misconduct, "spoil[ing] highly relevant evidence by, intentionally and in bad faith, concealing the existence of [her] Visa Card, [which] ... was highly prejudicial to [defendant], and ... never corrected***423** by [plaintiff]"); *accord United States v. Philip Morris USA Inc.,* 327 F.Supp.2d 21, 26 (D.D.C.2004) (holding that a fine of $2,995,000 payable to the Court Registry "is particularly appropriate here because [the Court has] no way of knowing what, if any, value [the] destroyed emails had to Plaintiff's case; [therefore] ... it [is] impossible to fashion a proportional evidentiary sanction that would accurately target the discovery violation.... [Yet], it is essential that such conduct be deterred ... and that the amount of the monetary sanction fully reflect the reckless disregard and gross indifference displayed by [defendants] toward their discovery and document preservation obligations"); *In re Prudential Ins. Co. of Am. Sales Practices Litig.,* 169 F.R.D. 598, 617 (D.N.J.1997) (imposing $1 million fine, payable to the Clerk of the U.S. District Court for the District of New Jersey, for Prudential's consistent pattern of document destruction, where Prudential violated a court order "on at least four occasions," "ha[d] no comprehensive document retention policy," and "impede[d] the litigation process"; reasoning that the fine "informs Prudential and the public of the gravity of repeated incidents of document destruction and the need of the Court to preserve and protect its jurisdiction and the integrity of the proceedings before it").

CONCLUSION

For the foregoing reasons, the Court holds that neither Passlogix nor 2FA has established by clear and convincing evidence that its adversary committed a fraud on the Court. 2FA's request to amend its counterclaims to assert a cause of action for malicious prosecution against Passlogix is denied on grounds of futility. The Court also holds that 2FA's failure to preserve relevant documents led to the spoliation of evidence in this case. Therefore, the Court hereby orders 2FA to pay a fine in the amount of ten thousand dollars ($10,000.00), via check made payable to "Clerk, U.S. District Court" within thirty (30) days from the date of this Opinion and Order.

708 F.Supp.2d 378
(Cite as: 708 F.Supp.2d 378)

SO ORDERED.

S.D.N.Y.,2010.
Passlogix, Inc. v. 2FA Technology, LLC
708 F.Supp.2d 378

END OF DOCUMENT

Not Reported in F.Supp.2d, 2013 WL 1701066 (E.D.Tenn.)
(Cite as: 2013 WL 1701066 (E.D.Tenn.))

H

Only the Westlaw citation is currently available.

United States District Court, E.D. Tennessee.
Barbara GILLEY, Plaintiff,
v.
ELI LILLY AND COMPANY, Defendant.

No. 3:10–CV–251.
April 2, 2013.

Adam U. Holland, Phillip E. Fleenor, Duncan, Hatcher, Hixson & Fleenor, PC, Chattanooga, TN, for Plaintiff.

Amy M. Steketee, Faegre Baker Daniels LLP, South Bend, IN, Ellen E. Boshkoff, Baker & Daniels LLP, Indianapolis, IN, Michael S. Moschel, Robert W. Horton, Bass, Berry & Sims, PLC, Nashville, TN, for Defendant.

REPORT AND RECOMMENDATION

H. BRUCE GUYTON, United States Magistrate Judge.

***1** This case is before the undersigned pursuant to 28 U.S.C. § 636, the Rules of this Court, and the referral of the District Judge. Defendant's Motion to Dismiss as Sanctions for Discovery Abuse and for Spoliation [Doc. 94] is pending before the undersigned. The parties appeared before the undersigned on March 8, 2013, to address the Motion to Dismiss and a motion *in limine* pending. Attorneys Adam Holland and Philip Fleenor were present representing the Plaintiff, and Attorneys Ellen Boshkoff and Michael Moschel were present representing the Defendant.

The Court has considered the parties' filings on this issue along with their oral arguments. For the reasons stated below, the undersigned will **RECOMMEND** that the Motion to Dismiss as Sanctions for Discovery Abuse and for Spoliation be **GRANTED IN PART** and **DENIED IN PART.**

I. BACKGROUND

Plaintiff was employed by the Defendant. Defendant terminated Plaintiff's employment in December 2008 because Plaintiff allegedly failed to complete a computer-based compliance training ("the Red Book training") on time, allegedly lied about it, and then allegedly falsified a completion certificate. In an attempt to prove she had completed the training by the deadline, Plaintiff faxed to Defendant, on December 12, 2008, and later sent via Federal Express two documents purporting to be training verification certificates indicating she had completed the training on November 10, 2008.

Lori Cochrane, a human resources representative for the Defendant, was suspicious of Plaintiff's claim to have such certificates. She contacted Defendant's training and compliance department to inquire about Red Book training procedures. Cochrane allegedly learned that the Red Book training program was only set up to capture an electronic signature and was not enabled to display a certificate of completion on the screen or to print out a certificate. Cochrane also allegedly learned that Plaintiff had not completed Red Book training until on or about December 6, 2008. Defendant states that the Plaintiff's employment was terminated, based upon this information, effective December 29, 2008.

Plaintiff maintains that she completed the Red Book Training on November 10, 2008, prior to the expiration of the deadline for doing so. [Doc. 95–1 at 9–10]. Plaintiff maintains that when she completed the training, a certificate of completion appeared on her screen, but it would not print out. *Id.* In her first de-

position, Plaintiff testified that she took a picture of the certificate with her own cell phone when the certificate would not print out. [Doc. 95–1 at 10]. She further testified that she transferred the picture with a USB cord to the printer and printed it. [*Id.*]. When asked if she still had that cell phone, Plaintiff replied: "I believe I do, yes." [*Id.*].

Following her first deposition, Defendant asked Plaintiff to produce the cell phone and allow Defendant to inspect the digital file. In response, Plaintiff advised Defendant that the cell phone with which Plaintiff had taken the photograph was no longer in her possession. [Doc. 95–5 at 4]. Plaintiff's counsel also responded:

> ***2** First, with respect to the request for the digital file of the Red Book Training Certificate, it is my understanding that the photo was taken by cell phone and was thereafter downloaded to the Plaintiff's company lap top computer via USB cable. The "digital file" would therefore be on Plaintiff's company lap top which was returned to Lilly at the time she was terminated. We do not have what was sent to Plaintiff's cell phone by the daughter on December 29, 2008.....
>
> Second, the cell phone used to photograph the Red Book Training Certificate was returned to Verizon Wireless after ordering a new cell phone. Plaintiff has been informed by Verizon Wireless that once the old cell phones are returned to the manufacturer, the manufacturer does a Master Reset, cleaning the phone of all data for re-sale purposes.....
>
> [Doc. 95–8 at 2].

As a result of Plaintiff's changed testimony regarding the cell phone, Defendant asked to take a follow up deposition of Plaintiff, which occurred on February 14, 2013. [*See* Doc. 95–1 at 14]. In the second deposition, Plaintiff testified she took two different photographs of the certificate: a photograph of the screenshot of the certificate with her cell phone ("Photo # 1") and with her daughter's cell phone ("Photo # 2"). [*Id.* at 23]. Plaintiff contends that she then connected her daughter's cell phone to the laptop issued to her by Defendant with a USB cable, downloaded the photograph from the cell phone, saved to her "desktop" folder on her laptop, and then printed the picture. [*Id.* at 26].

Plaintiff confirmed that retaining a copy of this photo was important and that was why she wanted a copy. [*Id.* at 27]. She testified that on December 12, 2008, she called or texted her daughter, confirmed that her daughter still had the photo of the certificate on her phone, asked her not to delete it, and asked her daughter to send it to her. Plaintiff stated that her daughter sent the photo to her Hotmail email address. [*Id.* at 34–35]. Plaintiff confirmed that on December 29, 2008, she sent the photo to Attorney David Burkhalter. She confirmed that the photo was sent from her Hotmail account. [*Id.* at 35]. Plaintiff stated that this Hotmail account has not been terminated and "still exists," but she asserted that she "can't get into it." [*Id.*]. She asserts that she does not know the password to a personal email account. [*Id.* at 33 (asserting that she lost the password to an email account)].

Defendant submits that according to Plaintiff's testimony, by December 29, 2008, there were at least six digital files of photographs of the purported training certificate that had been taken with either Plaintiff's cell phone or her daughter's cell phone, including: (1) the digital file on Plaintiff's cell phone of the photograph she took with own cell phone (*i.e.*, Photo # 1); (2) the digital file on Plaintiff's daughter's cell phone of the photograph taken with Plaintiff's Daughter's cell phone (*i.e.*, Photo # 2); (3) the digital file of Photo # 2 on saved on the laptop issued by Defendant; (4) the digital file on Plaintiff's cell phone or in her Hotmail email account of Photo # 2 sent to Plaintiff by her daughter on December 12, 2008; (5)

the digital file in Plaintiff's Hotmail email account of Photo # 2 sent to her attorney on December 29, 2008 of Photo # 2; and (6) the digital file in Plaintiff's attorney's email of the text and photograph he received from Plaintiff on or about December 29, 2008. Defendant maintains that Plaintiff has not produced any of these digital photos and apparently failed to preserve any of them.

***3** Two additional issues surfaced in early 2013. First, Plaintiff testified that there could be a "box of emails" relevant to the case that have yet to be produced. [Doc. 95–1 at 33].[FN1] Second, Plaintiff disavowed a document that she produced in discovery, which purports to be a certificate of completion of the training for the Red Book that is at issue in this case. [FN2]

FN1. On February 14, 2013, Plaintiff testified:

> Q: You started sending yourself a whole bunch of e-mails in November right before you were fired?
>
> A: Is there a problem with that?
>
> Q: They haven't been produced in discovery. Do you have an explanation for that?
>
> A: They're in a box somewhere, and I'm not the—I can't—I didn't—I can't go do this. I wasn't representing myself.
>
> Q: No, your obligation is to make sure that your lawyer has everything.
>
> A: He does have everything.
>
> Q: Okay. So we think there's a box of e-mails somewhere that haven't been produced?
>
> A: Yes.

FN2. An email sent by Adam Holland, counsel for the Plaintiff, states "Ms. Gilley does not recognize document PLF 436 and has no idea where it came from nor why it was produced by her counsel. She is adamant that the training test did not display a certificate entitled 'The Red Book Training', she stated to me that it simply stated 'The Red Book' when it appeared on her screen. Obviously you can ask here [sic] about this at her supplemental deposition tomorrow." [Doc. 95–14].

Thus, presently there are three issues pending before the Court: (1) the Plaintiff's failure to preserve and produce the digital files of the photos taken of the certificate of completion screen using Plaintiff's phone and her daughter's phone; (2) the additional "box of emails" that has not been produced; and (3) the Plaintiff's disavowing of the certificate of completion produced by Plaintiff, or her representative, in discovery and marked as PLF000436.

II. ANALYSIS

The Court will address each of these issues in turn, and the Court will incorporate the positions of the parties in the analysis of each issue.

A. Rule 37 of the Federal Rules of Civil Procedure

Rule 37 of the Federal Rules of Civil Procedure states:

> (c) Failure to Disclose, to Supplement an Earlier Response, or to Admit.
>
> (1) Failure to Disclose or Supplement. If a party fails to provide information or identify a witness as required by Rule 26(a) or (e), the party is not al-

> lowed to use that information or witness to supply evidence on a motion, at a hearing, or at a trial, unless the failure was substantially justified or is harmless. In addition to or instead of this sanction, the court, on motion and after giving an opportunity to be heard:
>
> (A) may order payment of the reasonable expenses, including attorney's fees, caused by the failure;
>
> (B) may inform the jury of the party's failure; and
>
> (C) may impose other appropriate sanctions, including any of the orders listed in Rule 37(b)(2)(A)(i)-(vi).

Fed.R.Civ.P. 37(c)(1). The sanctions listed in Rule 37(b)(2) (A)(i)-(vi), include: "(i) directing that the matters embraced in the order or other designated facts be taken as established for purposes of the action, as the prevailing party claims; (ii) prohibiting the disobedient party from supporting or opposing designated claims or defenses, or from introducing designated matters in evidence; (iii) striking pleadings in whole or in part; (iv) staying further proceedings until the order is obeyed; (v) dismissing the action or proceeding in whole or in part; [and] (vi) rendering a default judgment against the disobedient party." *Id.* (formatting modified).

In this case, the Defendant focuses, almost exclusively, upon the fifth of these sanctions: dismissing the action. When considering a dismissal as a sanction for discovery infractions, the Court must consider four factors, including whether: (1) the party's failure to cooperate in discovery is due to willfulness, bad faith, or fault; (2) the adversary was prejudiced by the party's failure to cooperate in discovery; (3) the party was warned that failure to cooperate could lead to the sanction; and (4) less drastic sanctions were first imposed or considered. *Freeland v. Amigo*, 103 F.3d 1271, 1277 (6th Cir.1997).

B. Plaintiff's Failure to Preserve Digital Images

***4** The Defendant maintains that the Plaintiff failed to preserve or produce any of the six digital images of the certificate. The Defendant argues that the Plaintiff failed to preserve these digital files, despite recognizing that they were "important." [Doc. 95 at 13]. Defendant argues that the Plaintiff cannot be excused from her duty to preserve and produce the digital images by casting blame on her former counsel. [*Id.*]. Defendant submits that this case turns on the legitimacy of the training certificate and the completion of the training. [*Id.* at 15]. Defendant contends that the digital images—more specifically, the metadata attached to the digital images—"could provide information regarding the precise date and time the photograph was taken and when it was saved to various locations." [*Id.* at 16]. Essentially, Defendant argues that, despite the fact that the digital images are the only original evidence of the Plaintiff's alleged receipt of a training certificate, the Plaintiff took no steps to preserve this critical evidence. [*Id.* at 1].

The Plaintiff does not dispute Defendant's contention that she did not preserve the photo images in their digital forms—*i.e.* as jpegs or similar digital format. The Plaintiff, instead, argues that she has produced these images as printed documents, and she implies that the printed versions of the images are sufficient. Plaintiff states that she has produced close to 1,000 pages of documents, including printed copies of the images. [Doc. 100 at 3]. Plaintiff does not deny that the photos were not produced in digital format or that she failed to preserve the photos in digital format. Rather, she posits, "Defendant has never requested in formal discovery that Plaintiff produce any digital pictures of the Red Book certificate." [*Id.* at 4]. Plaintiff maintains that she sent printed copies of the images at issue to the Defendants by fax and FedEx, in December 2008. [Doc. 100 at 4].

Initially, the Court finds that the Plaintiff's own testimony indicates that there were six digital images

of the certificate of completion that is alleged to have displayed on her computer screen upon completion of her Red Book training. Plaintiff does not dispute the assertion that she has failed to preserve any of these digital images. Thus, the Court finds that the Plaintiff failed to preserve six digital images of the certificate of completion.

The Court further finds that these images in their printed form are not equivalent to the images in their digital form. Plaintiff does not dispute that metadata, including the date and time the image was captured, are not available to the Defendant through the printed forms that have been provided to the Defendant. Moreover, the Court finds that this metadata has almost certainly been lost forever. It is important to note that, while it appears that the Plaintiff could possibly gain access to the Hotmail account through which the digital images were allegedly sent by contacting the operator of the email service, counsel for the Plaintiff *never* represented to the Court that the Plaintiff was prepared to present the digital images to opposing counsel or the Court.

***5** The Court finds that at least negligent destruction of evidence has occurred. With Rule 37 of the Federal Rules of Civil Procedure in mind, the Court turns to the case law of the Sixth Circuit to determine if this destruction constitutes spoliation.

The Court of Appeals for the Sixth Circuit has clarified that a federal court in the Sixth Circuit should apply federal law in determining whether spoliation sanctions are appropriate. *See Adkins v. Wolever*, 554 F.3d 650, 652 (6th Cir.2009). Under applicable federal law, the party seeking adverse inference must establish that: (1) the party with control over the evidence had an obligation to preserve it at the time it was destroyed; (2) the evidence destroyed was destroyed with a culpable state of mind; and (3) the destroyed evidence was "relevant to the party's claim or defense." *Beavan v. United States*, 622 F.3d 540, 553 (6th Cir.2010).

The Court of Appeals has implied that these same elements are applied in evaluating spoliation sanctions, other than requests for adverse inferences. *Id.* at 554. The district court may "impose many different kinds of sanctions for spoliated evidence, including dismissing a case, granting summary judgment, or instructing a jury that it may infer a fact based on lost or destroyed evidence." *Id.* (quoting *Adkins*, 554 F.3d at 653). A party's failure to preserve relevant evidence calls upon the court to craft an appropriate sanction considering where the behavior falls "along a continuum of fault-ranging from innocence through the degrees of negligence to intentionality." *Id.* at 653 (quoting *Welsh v. United States*, 844 F.2d 1239, 1246 (6th Cir.1988).

1. Plaintiff had Control and Obligation

The Court finds, first, that the Plaintiff was the party with control over the evidence and that she had an obligation to preserve it at the time it was destroyed. The Plaintiff has never disputed that she had control over the digital images. She apparently relinquished control to the phones on which Photo # 1 and Photo # 2 were stored on her own volition, and she now claims to not remember how to access her email to retrieve the other images. The Plaintiff's voluntary or grossly negligent relinquishing of control does not undermine the control that she had over these images during the relevant periods.

The Plaintiff certainly had a duty to preserve the digital images. The Plaintiff caused the digital images to be produced by her phone's camera and then by the camera on her daughter's phone precisely because she knew the images were important to her employment. She was terminated by the Defendant on or about December 24, 2008, less than six weeks after the photo of the certificate was allegedly first taken and less than two weeks after she asked her daughter to send the digital photo from the daughter's phone to the Plaintiff's email or phone. Moreover, on or about December 29, 2008, the Plaintiff forwarded the mes-

sage from her daughter containing the digital photo to Plaintiff's attorney. Plaintiff testified in her deposition that she took the digital photos because the Red Book test was "important." [Doc. 95–1 at 27].

***6** Further, Plaintiff had been in touch with David Burkhalter, who later served as counsel in this matter, as early as September 2008, with regard to allegations of discrimination on the part of Defendant. [Doc. 95–2 at 2–3]. The date on which Mr. Burkhalter was retained to represent Plaintiff in this litigation is the subject of dispute. [Doc. 95–1 at 34–35]. A signature, purporting to be the signature of the Plaintiff, is affixed to a Representation Agreement with Mr. Burkhalter dated December 24, 2008. [Doc. 95–2 at 20]. Plaintiff disavowed this date, [Doc. 95–1 at 34], but Plaintiff has testified that she sent at least one of the digital images at issue to Mr. Burkhalter on December 29, 2008, [*id.* at 35]. It is undisputed that he was retained no later than January 16, 2009. On January 16, 2009, Mr. Burkhalter sent a letter noting the doctrine of spoliation and directed the Defendant to immediately preserve *inter alia* texts and emails. [Doc. 95–2]. The Court finds that the Plaintiff knew or should have known that the digital images would be relevant to forthcoming litigation.

Under these circumstances, the Court finds that the Plaintiff had a duty to preserve the digital photos.

2. Plaintiff was Culpable Because She Either Knowingly or Negligently Destroyed the Evidence

The Court turns next to the issue of culpability. The Court of Appeals for the Sixth Circuit has held that "[a]n obligation to preserve may arise when a party should have known that the evidence may be relevant to future litigation, but, if there was no notice of pending litigation, the destruction of evidence does not point to consciousness of a weak case and intentional destruction." *Beaven*, 622 F.3d at 554 (internal quotations and citations removed). The culpable state of mind factor is satisfied by showing that evidence was destroyed knowingly or negligently, even without demonstrating intent to breach the duty to preserver. *Id.* (citing *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 107 (2d Cir.2002)); *see also Stocker v. United States*, 705 F.3d 225, 235 (6th Cir.2013).

Analysis of the Plaintiff's culpability overlaps, to a degree, with the Court's analysis of her duty to preserve the digital images above, and the Court incorporates the findings relating to Plaintiff's knowledge herein. In brief, the Court finds that the Plaintiff knew or had reason to know as soon as she took the photos with her phone in November 2008, that these photos could be relevant to future litigation. This knowledge was again demonstrated on December 12, 2008, when she asked her daughter to resend the digital photo because she wanted a "backup" of the photo, [Doc. 95–1 at 34], because it was important [*id.* at 35]. Perhaps most importantly, on December 29, 2008, Plaintiff sent the photo to counsel, and the Court finds that she thereby demonstrated that she knew—or at a minimum, should have known that—the evidence may be relevant to future litigation.

***7** Accordingly, the Court finds that the Plaintiff was culpable because she knew or should have known that the digital images could be relevant to future litigation. The Court, therefore, finds that the Plaintiff had a culpable state of mind.

3. The Evidence Destroyed is Relevant

Finally, the Court finds that the metadata that has been lost and the images in digital form are relevant evidence. The Plaintiff does not dispute this finding. The Court finds that the issues in this case turn on the dates and times that certain tasks—*i.e.* training on the Red Book—were completed. The digital images and metadata would have made the dates and times alleged by the parties "more or less probable" than they would have been without the evidence. *See* Fed.R.Evid. 401.

Accordingly, the Court finds that the digital im-

ages, which have been lost/destroyed, were relevant. Thus, the Court finds that: (1) the Plaintiff had control over the evidence and a duty to preserve it; (2) the Plaintiff had a culpable state of mind; and (3) the digital images that were lost/destroyed were relevant. The Court finds that the Plaintiff's arguments that Defendant did not formally request the digital images, or in the alternative, that the Defendant's request for relief is barred by undue delay are not persuasive or well-taken. Therefore, the Court finds a sanction based upon spoliation of evidence is appropriate.[FN3]

> FN3. The Court finds that the spoliation analysis, as guided by the case law of the Court of Appeals for the Sixth Circuit, correlates to and incorporates the factors for Rule 37 analysis outlined by the Court of Appeals.

4. An Instruction to the Jury Regarding Inferences, Combined with the Availability of Cross–Examination, is an Appropriate Sanction

The Court turns to the imposition of an appropriate sanction. As noted above the Court may "impose many different kinds of sanctions for spoliated evidence, including dismissing a case, granting summary judgment, or instructing a jury that it may infer a fact based on lost or destroyed evidence." *Beaven,* 622 F.3d at 554.

The Defendant has suggested that dismissal of this action is an appropriate sanction. The Court finds that this sanction is too extreme a remedy for the Plaintiff's behavior. The Court of Appeals for the Sixth Circuit has indicated that dismissal is an appropriate spoliation sanction where a defendant has been denied the opportunity to develop its defenses adequately and/or when bad faith is found. *See Arch Ins. Co. v. Broan–NuTone, LLC,* 2012 WL 6634323 (6th Cir. Dec.21, 2012).

In this case, the Plaintiff has produced printed copies of the digital images at issue; thus, the Defendant has not been wholly denied access to the images. The Court recognizes that these printed copies deny the Defendant the metadata and other relevant information that could have been provided through the digital images. Nonetheless, the Defendant will have the opportunity to cross-examine the Plaintiff about the printed copies, which are inconsistent with one another, and the Defendant will have the opportunity to ask the Plaintiff, in front of the jury, why the digital images were not preserved. Moreover, the Court cannot find bad faith on the facts before it. Accordingly, the Court finds that dismissal is not an appropriate sanction.

***8** In fashioning a lesser sanction, the Court has considered an array of case law relating to spoliation generally and spoliation of digital images and documents specifically.

The Court finds *Arch Insurance Co. v. Broan–NuTone, LLC,* 2012 WL 6634323 (6th Cir. Dec.21, 2012), to be instructive. In *Arch Insurance,* plaintiffs filed a subrogation action in September 2009, relating to a fire at a municipal fire station. As early as October 17, 2007, one month after the fire, an insurance adjuster had opined that the fire was caused by an exhaust fan. *Id.* at *2. The exhaust fan was inspected by an engineering company. Thereafter, a third-party administrator received an invoice from the engineering company charging a fee for continued storage. *Id.* To minimize costs, the third-party administrator gave permission for the exhaust fan to be destroyed without consulting either the plaintiff or the defendant. *Id.* The district court concluded that a permissive adverse-inference instruction was the appropriate sanction for this spoliation. *Id.* at *3.

The Court of Appeals for the Sixth Circuit in *Arch Insurance* found that the district court's use of a permissive adverse-inference instruction as a sanction was not an abuse of discretion. *Id.* at *5. In so deciding, the Court of Appeals noted that defendant had

access to the exhaust fan before it was destroyed and was on notice of the plaintiff's general theory of recovery. *Id.* at *3. The Court of Appeals noted that a "permissive instruction is particularly appropriate if the evidence was not intentionally destroyed." *Id.* at *4 (citing *Blinzler v. Marriott Int'l, Inc.*, 81 F.3d 1148, 1159 (1st Cir.1996)). The defendant in *Arch Insurance* argued that the permissive instruction had no effect at all, but the Court of Appeals found that "the instruction came dressed in the authority of the court, giving it more weight than if merely argued by counsel." 2012 WL 6634323 at *5 (citing *Boyde v. California*, 494 U.S. 370, 384, 110 S.Ct. 1190, 108 L.Ed.2d 316 (1990)).

The Court also finds ***Christou v. Beatport**, LLC*, 2013 WL 248058 (D.Colo. Jan.23, 2013),[FN4] to be persuasive authority with regard to the appropriate punishment. In *Christou*, defendant took no steps to preserve text messages on his iPhone. *Id.* at *13. Defendant submitted that he had lost the phone and with it any text messages saved on it. *Id.* The court in *Christou* could not make a finding of relevancy based upon the evidence before it and had no "basis to assume that the loss of the phone was other than accidental." *Id.* at *14. Nonetheless, the Court found that it was appropriate to allow the opposing party to present a litigation hold letter and reference the failure to preserve at the trial and to allow the jury to make an appropriate inference. *Id.*

> FN4. The Court is aware that *Christou* was decided by a district court sitting in the Ninth Circuit. The Court has considered this persuasive authority, because as the Court of Appeals for the Sixth Circuit has noted, "Because earlier precedents in this circuit applied state law on spoliation, we look to other circuits for guidance in this inquiry." *Beavan*, 622 F.3d at 553.

The Court finds that a permissive adverse-inference instruction is the appropriate sanction in this case. The Court will instruct the jury that it may infer, but is not required to infer, that the Plaintiff did not take the digital photo of the certificate of completion at the time to which she has testified, based upon her failure to preserve the digital images and their accompanying metadata.

***9** In reaching this conclusion, the Court has weighed the fact that the Plaintiff was, at least, negligent in the destruction of the digital images, and as in *Arch Insurance* and *Christou*, the Court finds that this level of culpability does not support dismissal. In addition, the Court has considered the fact that the Defendant has access to printed copies of the digital images and the fact that the Defendant has been aware that these digital images existed since at least November 11, 2013. [Doc. 95–1 at 9].

Some members of the jury may be familiar with the ease with which digital images can be obtained and preserved, and the jury can consider the Plaintiff's failure to preserve the digital images of the certificate of completion. The Court finds that taking the jury's knowledge a step further and cloaking the jury's own potential inferences in the authority of the court will increase the deference afforded to the potential inference. The permissive adverse-inference instruction remedies any advantage that the Plaintiff may have gained through her spoliation, while at the same time allowing the jury to fulfill its role as fact finder. The Court finds that a mandatory adverse-inference instruction would be too strong a sanction under the circumstances.

The Defendant may submit suggested language for the permissive adverse-inference on or before **May 31, 2013,** and the Plaintiff will have up to and including **June 10, 2013,** to object to the language used. In addition, the Defendant will be allowed to cross-examine the Plaintiff regarding the spoliation of the digital images, employing the Plaintiff's inconsistent statements in her depositions for impeachment as appropriate. Further, the Defendant may introduce the

letter from Mr. Burkhalter dated January 16, 2009, conveying on behalf of the Plaintiff the need to preserve evidence, as relevant evidence at the trial of this matter.

B. The Additional "Box of Emails"

The Court turns next to the issue of the additional "box of emails." As noted above, on February 14, 2013, Plaintiff testified:

> Q: You started sending yourself a whole bunch of e-mails in November right before you were fired?
>
> A: Is there a problem with that?
>
> Q: They haven't been produced in discovery. Do you have an explanation for that?
>
> A: They're in a box somewhere, and I'm not the—I can't—I didn't—I can't go do this. I wasn't representing myself.
>
> Q: No, your obligation is to make sure that your lawyer has everything.
>
> A: He does have everything.
>
> Q: Okay. So we think there's a box of e-mails somewhere that haven't been produced?
>
> A: Yes.
>
> [Doc. 95–1 at 33].

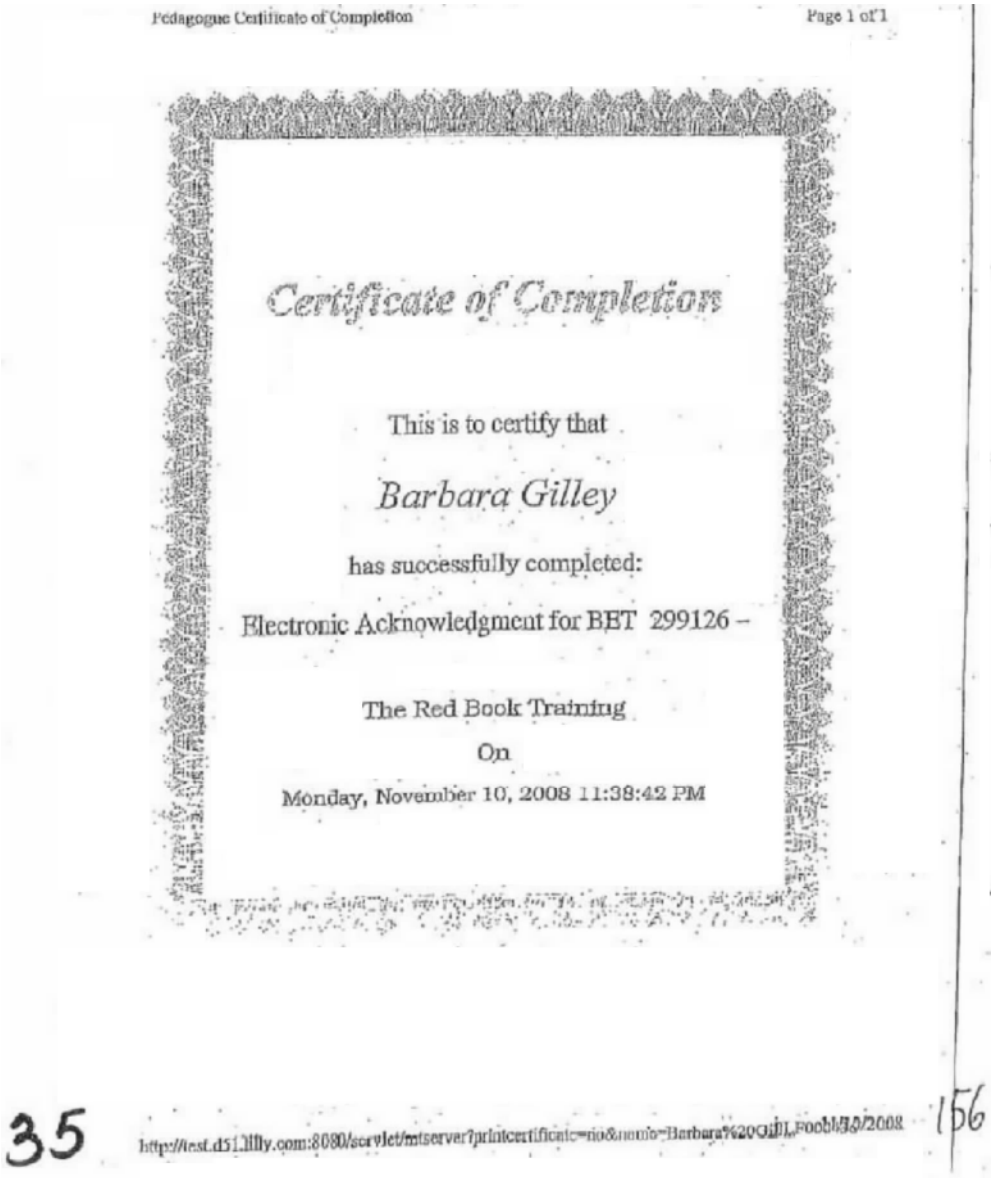
The date for producing these emails expired last year. The Court, however, finds that in the interest of adjudicating this matter on its merits, the Plaintiff will be afforded a final opportunity to produce these emails. The Plaintiff **SHALL PRODUCE** any and all relevant emails that are under her control. The Court interprets the term "under her control" to include any emails contained in email accounts held in Plaintiff's name, either personal or professional, to which the Plaintiff has access or the *ability* to obtain access. It is not enough for Plaintiff to say that she cannot recall her password or that she does not generally use an account any more. If Plaintiff asserts that she is *not able* to access an email account, she **SHALL SUBMIT** an affidavit stating the steps she has undertaken to obtain her password to the account or otherwise access the account. Plaintiff **SHALL PRODUCE *all*** relevant emails and/or any affidavit explaining non-production on or before **April 19, 2013.**

***10** Further, the Court unequivocally **ORDERS** that the Plaintiff shall produce any relevant evidence under her control on or **April 19, 2013.** This is an all-inclusive order directing that any discoverable evidence, in any form that it might take, be produced on April 19, 2013. Failure to produce any relevant discovery may result in the Court imposing the sanctions listed in Rule 37(b)(2), which include *inter alia* dismissal or "directing that ... designated facts be taken as established for purposes of the action."

Defendant will have up to and including **May 3, 2013,** to file any motions for spoliation or other motions related to this production, and Plaintiff will have up to and including **May 17, 2013,** in which to respond.

C. The Certificate of Completion, Marked as PLF000436

The Court turns next to the document referred to as PLF000436, which appears as follows:


Pedagogue Certificate of Completion Page 1 of 1

Certificate of Completion

This is to certify that

Barbara Gilley

has successfully completed:

Electronic Acknowledgment for BET 299126 –

The Red Book Training

On

Monday, November 10, 2008 11:38:42 PM

35 http://test.d51.lilly.com:8080/servlet/mtserver?printcertificate=no&name=Barbara%20Gilley&... 11/10/2008 156

[Doc. 95–15 at 37].

Defendant maintains that in February 2013, nearly three years into the instant litigation, the Plaintiff stated that she did not recognize this document. Defendant argues that providing false documents in discovery is a basis for sanctions. [Doc. 95 at 12]. Defendant contends that Plaintiff has admitted to submitting a fraudulent certificate, and Defendant argues that, absent some "cogent explanation for this discovery fraud," the alleged misconduct is grounds for dismissal. [*Id.*].

Plaintiff responds that she has produced a copy of the Red Book certificate, Document LLY–Gilley001926, she sent to Defendant by fax and Federal Express, and she has been questioned about the same. Plaintiff maintains that the Defendant will have an opportunity to cross-examine the Plaintiff regarding any inconsistencies between Document No. LLY–Gilley001926 and Document No. PLF000436.

[Doc. 100 at 2]. Plaintiff maintains that the discrepancies between these documents and Plaintiff's statement disavowing Document No. PLF000436 are not grounds for dismissal.

Defendant appears to lodge its request for discovery sanctions pursuant to Rule 37(c) of the Federal Rules of Civil Procedure based upon a failure to provide information or supplement. Rule 37(c)(1) directs, "If a party fails to provide information ..., the party is not allowed to use that information ... at a trial, unless the failure was substantially justified." In addition, Rule 37(c)(1) that as an alternative sanction the court may impose other appropriate sanctions under subpart (b)(2)(A) of Rule 37. These sanctions may include dismissal. *See* Fed.R.Civ.P. 37(b)(2) (A).

As noted above, the Court must consider four factors in evaluating a request to impose sanctions, including dismissal, under Rule 37. As noted above, these factors are whether: (1) the party's failure to cooperate in discovery is due to willfulness, bad faith, or fault; (2) the adversary was prejudiced by the party's failure to cooperate in discovery; (3) the party was warned that failure to cooperate could lead to the sanction; and (4) less drastic sanctions were first imposed or considered. *Freeland*, 103 F.3d at 1277.

***11** Initially, the Court finds that the Plaintiff's disavowal of Document No. PLF00436 is a failure to supplement under Rule 37, and thus, the Court turns to fashioning an appropriate remedy.

Applying the relevant factors, the Court finds that the Defendant has demonstrated that the Plaintiff's disavowal of Document No. PLF00436 was her fault. The Court, however, cannot find bad faith. The Defendant's brief does not cite the Court to facts supporting such a finding. The Court finds that this first factor weighs in favor of awarding a sanction, though not necessarily a sanction of dismissal.

Turning to the second factor, the Court finds that the Defendant was prejudiced by the Plaintiff's disavowal. On February 13, 2013, counsel for the Plaintiff wrote to counsel for the Defendant:

> Ms. Gilley does not recognize document PLF 436 and has no idea where it came from nor why it was produced by her counsel. She is adamant that the training test did not display a certificate entitled "The Red Book Training", she state to me that it simply stated "The Red Book" when it appeared on her screen. Obviously you can ask here [sic] about this at her supplemental deposition tomorrow.

[Doc. 95–14 at 2]. Counsel for the Plaintiff sent this email at 3:26 p.m. on the day before the supplemental deposition. The Court finds that the last minute disavowal of Document No. PLF00436 prejudiced the Defendant in its preparations for the supplemental deposition. The Court finds that this second factor weighs in favor of imposing a sanction.

Turning to the third factor, the Court finds that the Defendant has not directed the Court to any Order of the Court warning the Plaintiff that this type of behavior or failure to cooperate generally would lead to sanctions. The Court finds that the third factor does not weigh in favor of imposing a sanction.

With regard to the fourth factor, the Court finds that lesser sanctions have not been imposed and are likely to be effective. The Defendant concedes that lesser sanctions have not been imposed, but the Defendant argues that the disavowal could not be remedied through a lesser sanction. The Defendant's argument was based in part on the fact that at the time of briefing this case was set for trial on March 18, 2013. On March 14, 2013, the trial of this matter was reset to July 22, 2013. The Court finds that this additional time allows for lesser sanctions. The Court finds that the fourth factor weighs in favor of imposing a sanction other than dismissal.

Based upon the foregoing, the Court finds that sanctions should be imposed against the Plaintiff based upon her disavowal of Document No. PLF00436. The Court has considered the violation and failure to disclose in the context of this case, and the undersigned **RECOMMENDS** that the Plaintiff be sanctioned as follows:

1. Plaintiff **SHALL** sit for a third deposition, not longer than three (3) hours, between **May 20 and May 30, 2013;**

***12** 2. Plaintiff **SHALL** bear all costs and expenses—including attorneys' fees incurred by the Defendant, court reporter costs, and transcription costs—incurred in taking this third deposition;

3. All costs and expenses **SHALL** be paid to the appropriate vendors on or before **June 14, 2013;**

4. Defendant may question Plaintiff about Document No. PLF00436 at the trial of this matter, citing to any previous deposition testimony for impeachment; and

5. The Court will instruct the jury that: (1) a party has a duty to produce documents in discovery in good faith and (2) when a party is represented by counsel, counsel's actions are imputed to that party. The Defendant may submit suggested language for these instructions on or before **May 31, 2013,** and the Plaintiff will have up to and including **June 10, 2013,** to object to the language used.

III. CONCLUSION

In sum, the undersigned finds that the Motion to Dismiss as Sanctions for Discovery Abuse and for Spoliation is well-taken in part, and for the reasons stated herein, the undersigned **RECOMMENDS**[FN5] that it be **GRANTED IN PART** and **DENIED IN PART.** The undersigned **RECOMMENDS** that the Plaintiff be **SANCTIONED** as stated above and the parties be **ORDERED** to comply with the dates and deadlines set out in this Report and Recommendation.

FN5. Any objections to this Report and Recommendation must be served and filed within fourteen (14) days after service of a copy of this recommended disposition on the objecting party. Fed.R.Civ.P. 72(b)(2). Such objections must conform to the requirements of Rule 72(b), Federal Rules of Civil Procedure. Failure to file objections within the time specified waives the right to appeal the District Court's order. *Thomas v. Arn*, 474 U.S. 140, 106 S.Ct. 466, 88 L.Ed.2d 435 (1985). The district court need not provide *de novo* review where objections to this report and recommendation are frivolous, conclusive or general. *Mira v. Marshall*, 806 F.2d 636 (6th Cir.1986). Only specific objections are reserved for appellate review. *Smith v. Detroit Federation of Teachers*, 829 F.2d 1370 (6th Cir.1987).

E.D.Tenn.,2013.
Gilley v. Eli Lilly and Co.
Not Reported in F.Supp.2d, 2013 WL 1701066 (E.D.Tenn.)

END OF DOCUMENT

Not Reported in F.Supp.2d, 2013 WL 248058 (D.Colo.), 2013-1 Trade Cases P 78,230
(Cite as: 2013 WL 248058 (D.Colo.))

H

United States District Court,
D. Colorado.
Regas CHRISTOU, R.M.C. Holdings, L.L.C. d/b/a The Church, Bouboulina, Inc. d/b/a Vinyl, Molon Lave, Inc. d/b/a 2 A.M., City Hall, LLC, 1037 Broadway, Inc. d/b/a Bar Standard f/k/a The Shelter, 776 Lincoln St., Inc. d/b/a Funky Buddha Lounge, and 1055 Broadway, Inc. d/b/a The Living Room, Plaintiffs.
v.
BEATPORT, LLC, Bradley Roulier, and BMJ & J, LLC d/b/a Beta Nightclub and Beatport Lounge, Defendants.

Civil Action No. 10–cv–02912–RBJ–KMT.
Jan. 23, 2013.

Dale R. Harris, John Allen Francis, Kenzo Sunao Kawanabe, Davis Graham & Stubbs, Llp, Denver, Co, Jeffrey S. Vail, The Law Office Of Jeff Vail Llc, Englewood, CO, for Plaintiffs.

Kenzo Sunao Kawanabe Davis Graham & Stubbs, LLP, Denver, CO, Judy Bradshaw Snyder, Katherine M.L. Pratt, Patrick Michael Haines, Berg Hill Greenleaf & Ruscitti, LLP, Joe L. Silver, Martin Dean Beier, Silver & Deboskey, P.C., George Vernon Berg, Jr., Boulder, CO, for Defendants.

ORDER

R. BROOKE JACKSON, District Judge.

***1** This matter is before the Court on (1) Defendants' Motion to Exclude Plaintiffs' Expert Owen R. Phillips, Ph.D. [docket # 122]; (2) Plaintiffs' Motion for Sanctions for Spoliation [# 123]; (3) Defendants' Motion to Exclude Plaintiffs' Expert Witness Jay E. Freedberg [# 134]; (4) Defendant Beatport's Supplemental Motion for Sanctions Pursuant to Federal Rule of Civil Procedure 11 [# 137]; (5) Defendants' Combined Motion for Summary Judgment [# 148]; (6) Renewed Stipulated Motion to Set Dates Certain for Pre-trial Deadlines [# 174]; and (7) [Plaintiffs'] Unopposed Motion to Supplement Response to Motion to Exclude Jay E. Freedberg, CPA [# 189].

FACTS[FN1]

FN1. A more extensive recitation of the facts cans be found in the Court's order of March 14, 2012 which addressed defendants' motions to dismiss and a previous defense motion for sanctions.

In the 1990's Regas Christou founded several nightclubs in Denver's “South of Colfax Nightlife District.” Two of these nightclubs, The Church and Vinyl, developed national reputations as venues for “Electronic Dance Music” (sometimes referred to as “EDM”). Electronic Dance Music features live performances by disc jockeys who mix songs or “tracks” on expensive synthesizers and other computer based equipment and are viewed as artists in their own right. Each year DJ Magazine produces a list of the “Top 100” DJ's in the EDM world. These “A–List DJ's” command larger audiences and are in high demand by nightclubs. They also perform in other venues such as, in Colorado, the Ogden and Fillmore theaters and the Red Rocks amphitheater.

From 1998 to 2007 Bradley Roulier was employed by Mr. Christou as a “talent buyer.” As such, and apparently with considerable success, he assisted in booking A–List DJ's and other DJ's for Mr. Christou's clubs. Mr. Roulier and others also conceived of the idea of creating an online marketplace for promoting and selling (downloading) Electronic Dance Music. Mr. Christou liked the idea and provided both

financial and promotional support to Mr. Roulier and his partners. This idea led to the creation of Beatport in 2003. Beatport was enormously successful and has grown to become the largest online site that caters essentially exclusively to producers and consumers of Electronic Dance Music.

Anyone can download music from the Beatport website. However, the tracks sold on Beatport are designed especially for DJ's. They are free of Digital Rights Management or "DRM," which means they can be mixed and re-mixed on the types of equipment used by DJ's. They are meant to be played at loud volume on very expensive, high fidelity equipment that is available in the venues in which these DJ's work. Accordingly, the average cost of a single track is higher than tracks that can be downloaded on mass-market sites such as Apple's iTunes. Although many of the same DJ's do sell tracks on iTunes and various other online sites, Beatport considers itself to set the standard in the market that it serves.

In 2007 Mr. Christou and Mr. Roulier had a falling out, the cause of which is immaterial to the pending motions. Mr. Roulier left Mr. Christou, and in 2008 he founded his own competing club called Beta in the Lower Downtown area of Denver. The gist of the present suit is plaintiff's claim that Mr. Roulier has been threatening A–List DJ's that their tracks will not be promoted on Beatport if they perform in Mr. Christou's clubs, and as a result, Beta has largely taken over the Denver market.

PROCEDURAL HISTORY

***2** Plaintiffs filed this lawsuit on December 1, 2010. They originally asserted nine claims for relief: (1) illegal tying in violation of section one of the Sherman Act against all defendants; (2) monopolization (section two of the Sherman Act against defendants Beta and Mr. Roulier; (3) attempt to monopolize against Beta and Mr. Roulier; (4) conspiracy to monopolize against all defendants; (5) conspiracy to eliminate competition by unfair means in violation of section one of the Clayton Act; (6) theft of trade secrets; (7) violation of the Racketeer Influenced and Corrupt Organizations Act; (8) intentional interference with prospective business expectancies against Mr. Roulier; and (9) civil conspiracy against all defendants.

In its order of March 14, 2012 [# 146] the Court dismissed the RICO claim and found that that Mr. Christou personally lacked standing to assert the antitrust claims. With those exceptions, however, the Court denied the motions to dismiss. It also denied defendants' motion for sanctions.

Defendants filed their motion for summary judgment on March 15, 2012. The Court heard oral argument on summary judgment on July 11, 2012. However, plaintiffs' claims rested in part on the testimony of expert witnesses. Defendants had filed "Daubert" motions challenging the admissibility of the experts' opinions, and they requested an evidentiary hearing on those motions. That hearing was held on January 15, 2013. The Court now is in a position to rule on those motions, the summary judgment motion, and the other pending motions.

I. THE DAUBERT MOTIONS.

A. *Rule 702.*

Federal Rule of Evidence 702 provides,

> A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion if: (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue; (b) the testimony is based on sufficient facts or data; (c) the testimony is the product of reliable principles and methods; and (d) the expert has reliably applied the principles and methods to the facts of the case.

Not Reported in F.Supp.2d, 2013 WL 248058 (D.Colo.), 2015-1 Trade Cases P 78,230
(Cite as: 2013 WL 248058 (D.Colo.))

Thus, Rule 702 assigns the trial judge "the task of ensuring that an expert's testimony both rests on a reliable foundation and is relevant to the task at hand." *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 597 (1993). An opinion is *reliable* if the witness is qualified to give it, and it is based upon reliable scientific principles and sufficient facts. The Court may consider such factors as whether the expert's theories or methods can be tested; whether they have been subjected to peer review and publication; whether there is a known error rate; and whether they have gained a degree of acceptance in the relevant community. *Daubert*, 509 U.S. at 593–94. Opinions are *relevant* if they will be of assistance to the jury, that is, is there a "fit" or logical relationship between the proffered testimony and the factual issues in the case.

***3** The objective of *Daubert's* gatekeeping requirement is "to make certain that an expert, whether basing testimony upon professional studies or personal experience, employs in the courtroom the same level of intellectual rigor that characterizes the practice of an expert in the relevant field." *Kumho Tire Co., Ltd. v. Carmichael*, 526 U.S. 137, 152 (1999). The plaintiff need not "prove that the expert is undisputably correct or that the expert's theory is 'generally accepted' in the scientific community. Instead, the plaintiff must show that the method employed by the expert in reaching the conclusion is scientifically sound and that the opinion is based on facts that satisfy Rule 702's reliability requirements." *Goebel v. Denver & Rio Grande Western R. Co.*, 346 F.3d 987, 991 (10th Cir.2003) (internal citations omitted). However, the Court is mindful that Rule 702 was intended to create a liberal standard for the admissibility of expert testimony, not to create new barriers. *See Cook v. Rockwell Intern. Corp.*, 580 F.Supp.2d 1071, 1082 (D.Colo.2006).

B. *Defendants' Motion to Exclude Plaintiffs' Expert Witness Owen R. Phillips, Ph.D.* [# 122].

Dr. Phillips' opinions are expressed in his report of August 31, 2011 [# 122–3]. He was deposed on November 3, 2011 [# 122–4]. His opinions were criticized in the report of an expert engaged by the defendants, Dr. James A. Langenfeld, dated November 18, 2011 [# 122–15]. Dr. Phillips then prepared a rebuttal to the Langenfeld critique, issued on December 21, 2011 [# 122–5]. Both experts testified at length during the Daubert hearing on January 15, 2012.

In brief summary, Dr. Phillips' opinions are as follows:

1. The relevant tying market is "digital downloads of DRM-free, high fidelity Electronic Dance Music suitable for playing on high-performance sound systems globally (digital download market)."

2. The relevant tied market (also the market that defendants are attempting to monopolize) is "live performances by A–List DJs playing Electronic Dance Music at nightclubs in the Denver metro area (A–List DJ market)."

3. Beatport has very significant market power, amounting either to monopoly power or near monopoly power, in the digital download market.

4. Mr. Roulier, who has an ownership interest in Beatport, leveraged Beatport's market power in the digital download market to coerce A–List DJ's to perform at Beta and not to perform at The Church or Vinyl when they accepted night club gigs in Denver.

5. The tie-in arrangement has helped to give Beta a monopoly or near monopoly in the A–List DJ market.

6. This has caused damage to competition for A–List DJ's which has harmed both the DJ's and the patrons of Electronic Dance Music performances in

Denver nightclubs.

7. The defendants' anticompetitive behavior has caused The Church and Vinyl to experience significant revenue declines on the evenings they devote to Electronic Dance Music performances.

***4** *See* Report [# 122–3] at 8–9.

Reliability.

Dr. Phillips' qualifications were not contested. Briefly, he received his Ph.D. in economics from Stanford University in 1980. He has taught and done research in antitrust economics for more than 25 years, presently as a Professor of Economics and Associate Dean of the College of Business at the University of Wyoming. He has also been a visiting professor at the Harvard Business School, and he has worked as an economist at the Antitrust Division of the Department of Justice. He has published 23 peer-reviewed articles on antitrust economics. He has frequently served as an expert witness in federal courts in Colorado and elsewhere.

The point of beginning in the analysis of a tying or a monopoly claim is identification of the relevant markets in which the defendant operates. *See Telecor Communications, Inc. v. Southwestern Bell Telephone Company,* 305 F.3d 1124, 1130 (10th Cir.2002). Ultimately the determination of the relevant market or markets is a question of fact. *Id.* at 1131. The primary focus of defendants' motion to exclude Dr. Phillips' testimony is on his opinions regarding the relevant markets.

Dr. Phillips testified that antitrust economists use three methods to define the relevant market: (1) a formal study of cross-price elasticity; (2) the Small but Significant and Non-transitory Increase in Price ("SSNIP") test developed by the United States Department of Justice and the Federal Trade Commission in 1982 and incorporated into their *Horizontal Merger Guidelines;* and (3) the application of "practical indicia." The latter test stems from *Brown Shoe v. United States,* 370 U.S. 294 (1962). The Court identified seven factors that are examples of practical indicia that can be used to determine the boundaries of a submarket within a product market: (1) industry or public recognition of the submarket as a separate economic entity; (2) the product's peculiar characteristics and uses; (3) unique production facilities; (4) distinct customers; (5) distinct prices; (6) sensitivity to price changes; (7) specialized vendors. The *Brown Shoe* factors have been recognized as being relevant to the determination of primary markets as well as submarkets. *See, e.g., In re Live Concert Antitrust Litigation,* 247 F.R.D. 98, 124 (C.D.Cal.2007).[FN2]

FN2. Although this case arose in the context of a class certification dispute, it contains an excellent discussion of several antitrust principles in a factual setting somewhat akin to that presented here. I nevertheless might not have singled out a California district court's decision when the menu of Tenth Circuit and Supreme Court decisions is quite full but for the fact that defendants not only urged me to read it but to use it as a model for decision.

Although Dr. Phillips had a great deal to say about interchangeability of products and cross-elasticity of demand, he did not perform a formal study of cross-elasticity. He states that "economists are rarely given the opportunity to observe a significant price increase (*e.g.*, on the order of 5%), by a firm or group of firms from which a change in sales and profits can then be measured." Report [# 122–3] at 10. He therefore considers cross-price elasticity to be difficult to study. Based upon the reading I have done, that view is not unreasonable.

Dr. Phillips did apply both of the other methods in reaching his relevant market definitions. Defendants do not quarrel with the reasonableness of either of the

two methods. Dr. Phillips' testimony during the Daubert hearing featured a series of PowerPoint slides that he used to explain his application of the SSNIP test and *Brown Shoe's* seven practical indicia to specific facts that he obtained from cited documents, deposition testimony and interviews.

***5** I will not attempt to discuss in detail the facts and analysis that are set forth in a 43–page report (66 including exhibits), a 22 page rebuttal report, and approximately two and one half hours of hearing testimony. However, with respect to the "Digital Download Market," key facts on which Dr. Phillips relies include the following.

• Beatport is the largest online site that caters exclusively to Electronic Dance Music, particularly to DJ's who buy and sell EDM tracks and albums on line.

• Apple's iTunes is a much larger online source of music downloads. However, Mr. Roulier and others distinguish Beatport from iTunes on several grounds. Beatport's tracks have always been DRM-free; iTunes did not begin offering a DRM-free format until 2009. Beatport offers tracks in MP3, MP4 and WAV formats, the latter being the highest quality preferred by some DJ's and clubs; iTunes does not offer WAV format. Beatport offers 19 specialized music genre classifications tailored to nightclub performances. Beatport is often the first vendor to offer new music. It offers numerous exclusive tracks that DJ's want to make their sets unique. Beatport has a strategic partnership with the German company, Native Instruments GmbH, which manufactures the dominant hardware system used by DJ's. Beatport's tracks tend to be longer. Significantly, tracks downloaded from iTunes range from 69 cents to $1.29. A newly released exclusive track is priced by Beatport at $2.49. Nonexclusive tracks are generally priced at $1.99 (classic) and $1.39 (general). Tracks download as WAV files cost $1.00 more than these prices.

• Notwithstanding the higher prices, Beatport has been a huge commercial success. In 2010 it had 1.8 million registered users, and it claims to have more than two million monthly visitors. Its revenues have increased from $274,973 in 2004 to $39,263,871 in 2010. Beatport estimates that it has an 80% share of EDM downloads worldwide.

• According to an internal analysis, Beatport believes that it competes in a distinct market from the sales of digital music downloads on iTunes and other mass-market vendors. It considers its competitors in its market to be Juno Downloads, Traxsource, Trackitdown, DJ Download Satellite Records, What People Play, and Stompy.

• Dr. Phillips cites statements from several DJ's and others who recognize Beatport's market power and Beatport's ability to wield that power to accomplish its objectives.

• Because Beatport competes online, the geographic market is worldwide.

With respect to the A–List DJ market, both parties cite DJ Magazine's annual list of the top 100 DJ's as defining the category. Dr. Phillips accepts that definition. In reaching his opinions regarding the A–List DJ market, Dr. Phillips cited the following facts among others:

• Statistics compiled for the years 2006 through 2010 at The Church and Vinyl, and for 2008 through 2010 for Beta, show that A–List DJ's receive significantly higher compensation for a single performance than unranked DJ's.

***6** • A–List DJ's attract larger crowds, and nightclubs charge higher cover charges when the top DJ's perform.

• Although top DJ's perform at venues other than nightclubs, concerts generally have seated audiences as compared to nightclubs where a dance floor is the focal point. Consumers generally purchase relatively expensive concert tickets in advance; nightclubs charge cover charges that are generally less expensive and cater to "spur of the moment" decisions by not requiring advance reservations. Concert venues generally are open to everyone; nightclubs, which offer alcohol and appeal to single adults, have age restrictions. Nightclub patrons can get "up close and personal" with the celebrity DJ's. Altogether, nightclubs are a difference experience and attract a different crowd.

• In 2006 and 2007, i.e., before Beta opened, The Church and Vinyl combined averaged more than 40 performances by A–List DJ's per year. From 2008 through 2010 they averaged one or two A–List DJ performances per year. Beta averaged between 22 and 29 performances by A–List DJ's per years during 2008 through 2010.

• There is anecdotal evidence that A–List DJ's and their representatives recognize the importance of promotion on Beatport to their success, and that Mr. Roulier and Beatport have used Beatport's market power to pressure them to book performances at Beta and not to perform at The Church or Vinyl.[FN3]

FN3. Some of the anecdotal evidence relied upon by plaintiffs is in the form of recorded telephone calls, during which a DJ or representative of the DJ made statements to the effect that they were threatened with lack of promotion on **Beatport** unless they avoided the **Christou** clubs and played at Beta when in Denver. These individuals apparently do not reside within the subpoena power of this Court. Apparently they have not been deposed and might not, despite the parties' reputations and clout in the industry, be willing voluntarily to testify at trial. Defendants argue that the recorded statements are inadmissible hearsay. Judge Nottingham discussed somewhat similar evidentiary issues in *Nobody in Particular Presents, Inc. v. Clear Channel Comm'ns* ("*NIPP*"), 311 F.Supp.2d 1048, 1095–96 (D.Colo.2004). His comments suggest a view that e-mail messages showing persons agreeing to a tying arrangement were not hearsay but were "verbal acts." He also addressed the coconspirator exception to the definition of hearsay and the present sense impression exception to the hearsay rule. The parties' positions on these evidentiary rules did not receive much analysis in their various briefs. I am not suggesting or requesting motions in limine. I am simply suggesting that the parties take a hard look at these issues.

• Patrons are thought to be willing to travel up to 100 miles for entertainment. In any event, the three nightclubs in Denver are the only nightclubs presently offering live performances by A–List DJ's of Electronic Dance Music in Colorado.

Unsurprisingly, Dr. Phillips testified, in response to leading questions, that his opinions were based upon sufficient facts and data.

In their 62–page motion, defendants express numerous criticisms of Dr. Phillips' methods and conclusions. These criticisms were amplified in the report and testimony of the defendants' antitrust economics expert, Dr. Langenfeld. He, like Dr. Phillips, is a Ph.D. economist. He currently is a Managing Director and Principal of the Chicago consulting firm of Navigant Economics as well as an Adjunct Professor at the Loyola University Law School. He has impressive professional experience at the Federal Trade Commission and elsewhere; an extensive list of publications on antitrust and economics topics; many and substantial expert witness experience. His qualifications to express opinions in the field of antitrust eco-

nomics have not been challenged.

Dr. Langenfeld accuses Dr. Phillips of admitting that he developed his "Digital Download" market "in order to generate a sufficiently high market share necessary to support the claims in this case." Report [# 122–15] at 22. He cites Dr. Phillips' deposition at page 123 for that statement. I have reviewed the deposition testimony and find that this is not a fair interpretation of what Dr. Phillips said. Aside from that unfortunate misstep, however, there were a number of points of professional disagreement between the two men as to which reasonable minds could differ.[FN4] Suffice it to say that I have carefully considered Dr. Langenfeld's lengthy report, including his exhibits, and his testimony.

> FN4. One point that Mr. Langenfeld emphasizes to some extent and that defendants' brief emphasizes even more is that "downloads" are the wrong market; the key to Beatport's power is access and promotion. I do not find that there is actual disagreement. Mr. Phillips agrees that Beatport's ability to promote or withhold active promotion of a DJ's tracks, albums and charts is what gives it power. Downloads are a means of measuring market share and can be said to be a measure of successful promotion. *See* Phillips Rebuttal Report [# 122–5] at 8.

***7** I have also considered Judge Wilson's comments on Dr. Phillips' opinions in *In re Concert Antitrust Litigation*, 247 F.R.D. at 124–27, 140–46, and Judge Nottingham's comments on Dr. Phillips' opinions in *NIPP*, 311 F.Supp.2d 1048, 1057–59, 1065, 1067, 1077, 1081–93, 1097, 1100–03, 1110–12, 1120. In both of these antitrust cases Dr. Phillips was retained by the plaintiff as an expert in antitrust economics.

In *NIPP*, as here, Dr. Phillips did not do a cross-elasticity study in defining the relevant market. Judge Nottingham concluded that such a study is not always necessary and noted that Dr. Phillips relied on recognized factors including economic data, industry materials, pricing data and public recognition of the market. *Id.* at 1120. The court did not formally rule on defendants' Daubert challenge, but it did find that Dr. Phillips' opinions were sufficiently reliable for admission on the issue of market definition under Daubert. *Id.* The court relied heavily and continually on Dr. Phillips' analysis throughout its opinion.

The court in *In re Concert Antitrust Litigation* did not conduct a Daubert analysis. 247 F.R.D. at 116 n.17. It criticized some of Dr. Phillips' opinions, just as it criticized some of the opinions of defendants' expert. At the Daubert hearing in the present case Dr. Phillips testified that while he did not agree with Judge Wilson's criticisms, he took them to heart and believes that he addressed the issues in his reports and opinions here, in particular, that he considered and applied all seven of the *Brown Shoe* practical indicia.

Ultimately, however, how Dr. Phillips' opinions fared in those cases does not determine the fate of his opinions here.

Relevance

"Relevant markets," a "tying product," a "tied product," "market power," "monopoly," "monopsony," and how those terms fit the facts of this case are largely beyond the ken of a typical lay juror. I have little doubt that the testimony of Dr. Phillips, and that of Dr. Langenfeld, will be of assistance to the jury in understanding the facts and the issues of this case. That is why the use of such experts is common in antitrust cases. These opinions are therefore relevant.

Conclusion

As indicated above, the Court's task is not to decide which expert is correct. Rather, it is to decide whether Dr. Phillips' opinions are so far divorced from

recognized science in his field, and so unsupported by facts, as to be unworthy of being heard at all. I conclude that he is highly qualified to render opinions in antitrust economics, and that his opinions are reliable and relevant within the meaning of Rule 702. Defendants' criticisms go to the weight to be given to his testimony by the jury, not to its admissibility. Accordingly, the motion to exclude his testimony is denied.

C. *Jay E. Freedberg.*

Mr. Freedberg is plaintiffs' damages expert. Like Dr. Phillips and Dr. Langenfeld, Mr. Freedberg has prepared a lengthy report. [# 134–2]. His opinions are that (1) because of the decline in A–List DJ performances after Beta opened, The Church and Vinyl suffered losses of profits on their respective Thursday and Saturday EDM nights in the amounts of $746,923 (The Church) and $422,621 (Vinyl); and (2) because of the reduction in profitability, plaintiffs lost $2,144,286 in the value of their business enterprise as at December 31, 2010.

1. *Lost Profits.*

Reliability

***8** Mr. Freedberg is a Certified Public Accountant who has additional certifications in business valuation and financial forensics. He is currently a Vice President, Director and Senior Analyst in the Denver firm of Shuster & Company. His qualifications have not been contested in this case. He does not purport to have expertise in antitrust matters, nor has he attempted to form opinions regarding the merits of plaintiffs' claims. Rather, his role was to attempt to determine what money damage the plaintiffs have sustained if liability and causation are otherwise proven.

There is nothing mysterious about the lost profits calculation. Mr. Freedberg first examined actual cover charge revenue realized by The Church and Vinyl on their respective EDM nights in 2006 and 2007. He then projected "expected" cover charge revenue for 2008 through 2010, essentially on the initial assumption that things would stay about the same. However, recognizing that the economic downturn during those years probably would have caused a decrease in cover charge revenues, he attempted to account for that, using North American Industry Classification System statistics for revenue changes in Colorado Bars, Nightclubs and Drinking Establishments during those years. He calculated historical (2006–2007) revenues from food, beverage and miscellaneous sales and assumed that that the average percentage of cover charge revenue from those years could be projected over the 2008 to 2010 period. This gave him "total revenue" projections for 2008 through 2010. Finally, he projected the two clubs' "variable expenses" (cost of goods sold, advertising, bank fees, equipment rent, payroll taxes) from the 2006–2007 experience to 2008 through 2010, and subtracted those projected expenses to determine "lost profit" during the three-year period.

In short, his methodology was, first, to project revenues that probably would have been realized had the business continued as in the past; next to account for factors unrelated to the case that probably would have impacted revenues; and finally to deduct projected expenses. Mr. Freedberg testified at the Daubert hearing that he used a methodology that is suggested by the American Institute of Certified Public Accountants in a technical practice aid. It is a methodology, he states, that is generally accepted in the accounting industry.

Defendants (including Dr. Langenfeld) do not take issue with the basic methodology, but they are critical of his application of the methodology in several respects. They contend that it is unreasonable to ignore revenue from other nights and from plaintiffs' other clubs and bars that offset the alleged losses on Thursdays at The Church and Saturdays at Vinyl. They challenge his failure to adjust for factors other than the economic downturn that might have reduced

revenues, such as the mere entry of a new and strong competitor in the market. They challenge his revenue projections, including his omission of 2005 revenue data. They question the conversion of lost sales on Thursday and Saturday nights to lost profits by the use of a variable cost to sales ratio estimated for all nights. They imply that Mr. Freedberg's reliance on information provided by plaintiffs' counsel raises questions about his numbers. In addition, during cross-examination defense counsel pointed out at least one mistake in his lost profits chart.

***9** Mr. Freedberg presumably can correct a mistake without materially changing his opinions. Whether he can provide reasonable and persuasive answers to the various other challenges defendants have raised is another matter.

Relevance

Calculation of lost profits is not something that a lay juror does on a daily basis. Mr. Freedberg's explanation of how he went about it would be of assistance to the jury.

Conclusion as to Lost Profits Testimony

I return to the core of what Daubert is about. No one questions Mr. Freedberg's credentials. His methods as such were not challenged. His work is essentially basic accounting. Mr. Langenfeld and defense counsel challenged certain assumptions and even mistakes in Mr. Freedberg's calculations. But there is no need for a gatekeeper to shield the jury from "junk science" or from someone who is out in left field, detached from the mainstream of his profession. His assumptions can be challenged on cross-examination and through expert testimony. Defendants' issues go to the weight, not the admissibility, of the opinions. The Court finds that the lost profits opinions are reliable and relevant within the meaning of Rule 702.

2. *Lost Enterprise Value*

Reliability

Mr. Freedberg testified that there are three commonly accepted methods to determine the value of a business: (1) calculation of net asset value; (2) comparable sales; and (3) the income method, i.e., capitalization of earnings. He did not use the net asset method, because it does not reflect good will, which he believes is a significant component of the value of plaintiffs' enterprise. He could not use the comparable sales method, because he could not identify any comparable sales. This is not surprising given that there are apparently only three nightclubs in Colorado that feature live performance by A–List DJ's of Electronic Dance Music. Defendants did not question the use of the capitalization of earnings method or even the capitalization rate that Mr. Freedberg used. *See* Langenfeld Report [# 122–15] at 58.

Relevance

A calculation of lost enterprise value, if otherwise relevant to the case, would be of assistance to the jury. The question in my mind is "fit," that is, whether there is a logical relationship between Mr. Freedberg's testimony regarding lost enterprise value and the factual issues in this case. The opinion as to the lost enterprise value as at December 31, 2010 seems, at least to me, to rest on two critical assumptions. First, that Mr. Christou intended to sell the two clubs in or about December 2010. Second, that events occurring after December 31, 2010 are not relevant.

With respect to the possibility of a sale in or about December 2010, plaintiffs have pointed to deposition testimony by Mr. Christou that he had had conversations with Mr. Roulier in the 2006–2007 time frame about Mr. Roulier's possibly buying The Church, and that they were "pretty close to the numbers." Deposition [# 14–6] at 72. He testified that Mr. Roulier suggested that Vinyl be turned into a condominium project, which he also thought was "not a bad idea." *Id.* at 72–73. This vague testimony, before Mr. Roulier left and formed Beta, does not say much about the

relevance of the value of Mr. Christou's clubs at the end of 2010.

***10** Moreover, even if it can be established that Mr. Christou did wish to sell at that time, is the alleged loss in enterprise value perpetual? What is the value of the enterprise today? If plaintiffs prevail, what happens to the value of the enterprise? Would damages for lost enterprise value as of December 31, 2010 permit Mr. Christou to have his cake and eat it too?

These questions were not answered during the Daubert hearing or in plaintiffs' brief. *See* Response [# 140] at 13–14. Recognizing that, plaintiffs have filed a motion to supplement their position regarding Mr. Freedberg's lost enterprise value opinion. [# 189] Defendants do not oppose this motion but "reserve their right" to file a response. Accordingly, motion # 189 is granted. The supplement provides authority for the common sense proposition that past lost profits and present lost enterprise value are not necessarily mutually exclusive. However, it does little to answer the questions in the Court's mind about the logical relationship between this opinion and the facts of this case. A response to this motion is not necessary.

Conclusion as to Lost Enterprise Value

Because I am not granting the motion to exclude Mr. Freedberg's testimony entirely, and because the basic questions I have raised have still not been addressed to my satisfaction, I elect to reserve judgment on the lost enterprise value opinion. If plaintiffs press this part of Mr. Freedberg's testimony, then I will decide whether to strike it in whole or part in the context of what is presented at trial. Suffice it to say at this point that I have my doubts.

II. SUMMARY JUDGMENT [# 148]

Summary judgment may be granted only if there is no genuine issue of material fact and the moving party is entitled to judgment as a matter of law. Fed.R.Civ.P. 56(a). Defendants filed an 82–page motion for summary judgment, supported by 39 exhibits that collectively comprised 676 pages of documents, on the day following the Court's denial of their motions to dismiss. It seeks dismissal of all of the plaintiffs' claims. Obviously this was not prepared overnight. It does not address the Court's analysis of the legal issues. For all these reasons, the motion is less helpful than it might have been. Nevertheless, I have read it, the response, and the reply. I have also reviewed the transcript of the oral argument.

A. *The Antitrust Claims.*

Defendants raise six groups of arguments as to why the antitrust claims should be dismissed:

1. *Plaintiffs' Cannot Prove Causation.* Motion [# 148] at 36–41.

Defendants argue that plaintiffs have not properly defined the relevant market. That reflects defendants' disagreements with Mr. Phillips' opinions, which I have held will not be excluded. Defendants argue that there is no proof that Beatport has sufficient market power to coerce or attempt to coerce A–List DJ's to shun Mr. Christou's clubs and play only at Beta. That turns on genuine and material fact disputes. Defendants argue that plaintiffs made the most profit ever in 2010 when they had the fewest performances by A–List DJ's. That begs the question whether the decrease in performances by A–List DJ's caused losses on Thursday and Saturday nights, notwithstanding successes in other areas of their business.

2. *Plaintiffs' Lack Standing. Id.* at 41–44.

***11** This was addressed by the Court in ruling on the motions to dismiss.

3. *Plaintiffs Have Not Presented Evidence Defining the Relevant Market. Id.* at 43–51.

This again gets back to defendants' disagreement with Dr. Phillips. The determination of the relevant markets is a question of fact. Whether Beatport had market or monopoly power in the alleged tying market

is a question of fact. Whether Mr. Roulier used Beatport's power to threaten and attempt to coerce A–List DJ's into playing at Beta rather than The Church or Vinyl if they performed in Denver is a question of fact. Whether the alleged tie-in succeeded and whether it was a cause of the decline in A–List DJ performances at Mr. Christou's clubs and the precipitous rise of such performances at Beta is a question of fact. Whether there was a conspiracy and, if so, who the conspirators were, are questions of fact. Whether Beta possesses monopoly power in the relevant market, and if so, whether that power was willfully acquired or maintained as distinguished from growth or development as a consequence of a superior product, *see United States v. Grinnell,* 384 U.S. 563, 570–71 (1966) are questions of disputed fact.

4. *Plaintiffs Cannot Show that Beatport had an Economic Interest in Requiring A–List DJ's to Perform at Beta. Id.* at 51–55.

This gets into the motives of Mr. Roulier, as a part owner of Beatport, and the relationship between Beatport and Beta, which plainly present issues of fact.

5. *Conspiracy Claims. Id.* at 55–59.

This essentially goes into whether Beatport, Beta and Mr. Roulier did conspire, or even legally can conspire, with each other. The former presents issues of disputed fact. The Court addressed the legal issue in its March 14, 2011 order.

6. *Attempt to Monopolize Fails as a Matter of Law. Id.* at 69–72.

Defendants argue that plaintiffs have no evidence of a dangerous probability that Beta will achieve a monopoly. Defendants suggest that there more than 400 drinking establishments in Denver, and that Beta accounts for just over one percent of the total revenues for such establishments. Alternatively, defendants suggest that there are approximately 32 nightclubs in Denver that play dance music, and Beta accounts for only three percent of the total number of nightclubs. As indicated above, the determination of the relevant market is a question of fact. Lumping Beta in with 400 drinking establishments or even other nightclubs who do not cater to patrons who seek out Electronic Dance Music, live performances by DJ's including A–List DJ's, complete with the high end equipment and sound that are features of the Christou and Roulier clubs, is questionable. In any event, it is not for a judge to determine the relevant market as a matter of law.

In short, the Court finds that the antitrust claims are riddled with fact disputes that are not susceptible to summary disposition.

B. *Misappropriation of Trade Secrets.*

***12** Defendants argue that the Sixth Claim, sounding in theft or misappropriation of trade secrets, should be dismissed as a matter of law. The Court addressed the legal issue in its order of March 14, 2012.

C. *Civil Conspiracy.*

Defendants argue that the civil conspiracy claims fail for the same reasons that the antitrust conspiracy claims fail. Motion [# 148] at 67. The antitrust conspiracy claims have not failed in the sense that the Court has declined to enter summary judgment dismissing them. The Court does question the necessity of clogging this case down with state law claims in view of the plain statement of plaintiff's counsel during the Daubert hearing that the strength of the case as plaintiffs view it is in their tying and attempt to monopolize claims.

Nevertheless, when one considers the elements of civil conspiracy under Colorado law—that (1) two or more persons (2) with an object to be accomplished (3) had a meeting of the minds on the object or a course of action (4) and took one or more overt acts (5) resulting in damages to the victim—it is evident that there are genuine issues of material fact in dispute that preclude summary disposition. Defendants argue that

"Plaintiff will tout a handful of ambiguous statements by Mr. Roulier and a variety of inadmissible statements by third-parties, who Plaintiffs did not bother to depose." *Id.* The ambiguity of Mr. Roulier's statements is for the jury to consider. Whether and to what extent plaintiffs will attempt to gain admission of third-party out-of-court statements remains to be seen, as does whether any or all of them might be admissible.

D. ***Lack of Subject Matter Jurisdiction.***

Defendants argue that if the federal claims were dismissed, the Court would no longer have "supplemental jurisdiction." I agree. They argue that there is no independent basis for jurisdiction, i.e ., diversity jurisdiction. I agree. However, so long as the antitrust claims continue, the state claims can tag along. It is tempting to decline supplemental jurisdiction and thereby simplify this case somewhat for the jury, the Court and even the parties. *See* 28 U.S.C. § 1367(c). However, that would create the risk of a new case in state court, thus continuing the economic debacle that has fallen on Mr. Christou and Mr. Roulier because of their stubborn refusal to get along. I find it to be better to try to resolve all their issues now.

E. ***Interference with Prospective Business Advantage.***

Defendants argue that this claim is time barred. They argue, and plaintiffs do not dispute, that the applicable period of limitations is two-years from the date plaintiffs knew of should have discovered all material facts essential to support the elements of the claim. This case was filed on December 1, 2010. However, among other things, plaintiffs received phone calls from DJ Rap in the summer and fall of 2008 [FN5] to the effect that she was being pressured by Mr. Roulier not to play at Mr. Christou's clubs. Defendants also cite to an email authored by Mr. Christou's talent buyer Jonathan Shuman dated October 30, 2008 [# 148–36] that contains a reference to "Lawsuit." *Id.* at 3.

FN5. Generally the defendants have taken the position that statements of that kind captured in recorded telephone calls constitute inadmissible hearsay. Presumably defendants offer this statement only as it relates to notice.

***13** Suffice it to say that the evidence cited by defendants does not clearly show that plaintiffs knew or should have known all material facts essential to support this claim. The jury will make that decision. Moreover, if one assumes that a common law claim of interference with plaintiffs' prospective advantage in terms of doing business with DJ Rap (who in any event appears not to have been an A–List DJ in 2008) were barred, it would not necessarily preclude a claim based on interference with plaintiffs' prospective advantage of doing business with A–List DJ's in 2009 and 2010, such as DJ Sharam and DJ Dan whom plaintiffs apparently tried to book in 2009.

Alternatively, defendants argue that plaintiffs cannot demonstrate a reasonable prospect of a business relationship with A–List DJ's during the relevant period. Plaintiffs point to DJ Sharam's deposition testimony that DJ Dan discussed the Denver situation, and that Mr. Roulier was (successfully) exerting pressure to avoid playing at Mr. Christou's clubs and to play only at Beta. [# 159–11] at 2–3. Both DJ Sharam and DJ Dan did play at Beta in 2009. [# 159–8] at 15, 16. This may not be overwhelming evidence, but it is enough to get by summary disposition.

III. OTHER PENDING MOTIONS

A. ***Plaintiffs' Motion for Sanctions for Spoliation [# 123].***

This case was filed on December 1, 2010. At or about that time plaintiffs served a "litigation hold letter" on the defendants, directing them to preserve

several categories of documents, including text messages. However, defendants took no steps to preserve the text messages on Mr. Roulier's iPhone. Defendants did not disclose any text messages in response to plaintiffs' first discovery requests served on May 19, 2011. In August 2011, according to Mr. Roulier, he lost his iPhone and with it any text messages saved on it. Plaintiffs contend that this "spoliation" of evidence should be sanctioned by an adverse jury instruction.

Defendants do not dispute that there were text messages on the phone or that those messages were lost with the phone. However, they note that Mr. Roulier has testified that he did not use text messages to book DJ's. Therefore, defendants argue, it is sheer speculation that his text messages contained relevant evidence. Further, defendants responded fully to the May 19, 2011 discovery, thus showing that there was nothing responsive in the text messages.

I agree that plaintiffs do not know whether the text messages contained, or even probably contained, relevant evidence. However, the fact that Mr. Roulier did not use texting to book DJ's is hardly proof that his text messages did not contain relevant evidence. Moreover, although defendants state that defendants "found no responsive text messages," they do not indicate that defense counsel reviewed Mr. Roulier's text messages and determined that they contained nothing of relevance. I note as well that the extensive motions practice that has characterized this litigation has revealed significant differences between the parties as to what is relevant and what is not. The point is that neither the plaintiffs nor the Court will ever know.

***14** Spoliation sanctions are proper when "(1) a party has a duty to preserve evidence because it knew, or should have known, that litigation was imminent, and (2) the adverse party was prejudiced by the destruction of the evidence." *Turner v. Public Serv. Co. of Colorado*, 563 F.3d 1136, 1149 (10th Cir.2009) (quoting *Burlington N. & Santa Fe Ry. Co. v. Grant*, 505 F.3d 1013, 1032 (10th Cir.2007)). Defendants had a duty to preserve Mr. Roulier's text messages as potential evidence, but they did not do it. Those text messages, few as they might have been, should have been preserved and either provided to the plaintiffs or potentially made the subject of further proceedings before the Court.

Nevertheless, the Court has no basis to assume that the loss of the phone was other than accidental, or that the failure to preserve the text messages was other than negligent. I agree that some sanction is appropriate. A commercial party represented by experienced and highly sophisticated counsel cannot disregard the duty to preserve potentially relevant documents when a case like this is filed. However, an adverse jury instruction is too harsh and is unwarranted as a sanction for the negligent "spoliation" of evidence in the circumstances presented here.

Accordingly, the Court grants the motion but orders as a sanction that plaintiffs will be permitted to introduce evidence at trial, if they wish, of the litigation hold letter and defendants failure to preserve Mr. Roulier's text messages. Plaintiffs may argue whatever inference they hope the jury will draw. Defendants may present evidence in explanation, assuming of course that the evidence is otherwise admissible, and argue that no adverse inference should be drawn.

B. *Beatport's Supplemental Motion for Sanctions [# 137].*

Beatport moved for Rule 11 sanctions against plaintiffs' counsel on February 7, 2012, arguing that none of the claims asserted in the Complaint were warranted by existing law or a nonfrivolous argument for extending, modifying or reversing existing law. They did so while their motion to dismiss was pending and before the Court addressed it. It turned out that for the most part Beatport's motion was denied on March 14, 2012. [# 146]. The Court denied the motion for sanctions and found that the filing of the motion was premature and reflected a lack of judgment. *Id.* at 33.

Ten days after filing its first motion for sanctions, but still before the Court issued its order on the motions to dismiss, Beatport filed a supplemental motion for sanctions [# 137]. The supplemental motion is 44 pages in length and makes numerous arguments.

First, defendants point to a surreptitiously recorded telephone conversation between Mr. Christou and gentleman named Scott Feiwell whom defendants describe as a "Las Vegas Promoter." *Id.* at 2. The call reflects a desire by Mr. Christou to "break" Mr. Roulier and Mr. Feiwell's suggestion that if he were to file a lawsuit, Beatport would knuckle under rather than fight it. Mr. Feiwell was full of advice, including that he include "restraint of trade, interstate commerce, defamation of character," perhaps 10 different things, and even throw in a racketeering claim, even though he might not be able to prove it. *Id.* at 3. Mr. Feiwell cautioned that the judge might dismiss some of the claims "right away," but what matters is that he would scare Mr. Roulier off. *Id.* Mr. Christou responded that if Mr. Feiwell would "get something like that (for) me," he would pursue it. *Id.* But, Mr. Christou asked, "Please, be quiet about it and you let me know and I will take care of you." *Id.* at 4.

***15** This telephone conversation reflects poorly on both men. Filing a lawsuit for the purpose of bringing the opponent to his knees because of the cost or distraction of the suit, as opposed to its merits, would be an abuse of the legal process. However, the fact remains that Mr. Christou retained excellent counsel, and counsel determined what claims to bring. Without any evidence I will not assume that these lawyers did not believe that there was a good faith basis in fact and law to sign the Complaint containing the claims asserted in it. The fact that the Court largely denied defendants' motion to dismiss, while not dispositive of Mr. Christou's allegedly improper motive, also tends to suggest that the claims did not lack a legal basis.

The Court did dismiss the RICO claim. A RICO claim by its nature is a severe charge, and such claims must be filed with caution and care. I do think that plaintiffs should have thought a little longer and harder before asserting RICO here. However, the Court did not find when it dismissed that claim, and does not find now, that it was so shallow as to be substantially groundless, frivolous or vexatious. I come back to my reliance on the good faith of counsel, which I do not override without demonstrable good cause. Just as I believe plaintiffs could have been more careful about asserting a RICO claim, I believe defendants should have been more cautious about accusing reputable counsel of incompetent and even unethical conduct.

Defendants find fault with the investigation conducted by plaintiffs' counsel, suggesting that counsel relied too heavily on the client for information. Again, however, defendants have provided nothing that suggests to this Court that plaintiffs' counsel either violated Rule 11 or otherwise failed to live up to their professional responsibilities. Defendants state that discovery has shown that some witnesses, including some DJ's, take issue with plaintiffs' recollection or interpretation of telephone conversations. That does not prove that the plaintiffs' versions are incorrect. In any event, there are recordings that do tend to support the plaintiffs' claims.

Defendants also fault plaintiffs for not consulting with Dr. Phillips before they filed this case. That may or may not have been wise. However, it appears to me that his analysis largely supports the claims in the Complaint, and I am not prepared to assume that this simply reflects that he is a "hired gun."

Defendants complain that Mr. Christou never sent Mr. Roulier a "cease and desist" letter, nor did he pick up the telephone and ask defendants to stop their alleged conduct. I agree that greater efforts probably

should have been made to resolve this dispute out of court. That can be said of many lawsuits. It does not make the filing of the suit sanctionable. To some extent this complaint is the stork calling the great blue heron stilted.

Defendants question the role of plaintiffs' other clubs, which they label the "coat-tail" plaintiffs, in this case. I do wonder about that. Unless plaintiffs have some reasonable ground for leaving those entities in the case, I suggest that they be voluntarily dismissed. The whole "South of Colfax Nightclub District" is relevant background, but the case appears to be about the three nightclubs that feature Electronic Dance Music.

***16** In sum, I do not find that the conduct of which defendants complain is sanctionable under Rule 11 or otherwise.

C. *Renewed Stipulated Motion to Set Dates Certain for Pre–Trial Deadlines [# 174].*

This is a joint motion to set pretrial deadlines that were not included in the magistrate judge's Final Pretrial Order issued May 15, 2012 [# 169] or the magistrate judge's Amended Minute Order issued May 24, 2012. The suggested dates for deposition designations are fine. However, before any deposition designations are filed, counsel should meet, confer, and exercise their best efforts to reduce deposition testimony to what is truly necessary and to resolve disputes. If there are disputes remaining, the Court will need hard copies with disputed portions designated and brief marginal notations indicating the parties' positions.

The Court does not wish to receive trial briefs. However, the Court requests that before the trial preparation conference on June 7, 2013 counsel will have done the following: (1) dismissed any claims and defenses that the party does not intend to pursue at trial; (2) exercised their best efforts to reach agreement on jury instructions; and (3) with respect to jury instructions as to which there is an unresolvable dispute, provide a brief indication of supporting authority. You should bring hard copies of such authority to the conference.

There is no need to submit preliminary or introductory instructions. The Court only wants instructions that would normally be given following the close of the evidence, i.e., an instruction describing the claims and defenses; the typical general instructions concerning burdens of proof, evidence, credibility, etc.; elements of claims and defenses; damages; a closing instruction briefly describing the deliberation process; and verdict form(s). If the parties and the Court can agree on a set of instructions at the trial preparation conference, the Court will instruct the jury before opening statements. In that event, the instructions will be given with the proviso that they are subject to revision, and that a final set of instructions will be given before closing arguments.

Order

1. Defendant's Motion to Exclude Plaintiff's Expert Owen R. Phillips [# 122] is DENIED.

2. Plaintiffs' Motion for Sanctions for Spoliation [# 123] is GRANTED. The sanction ordered is set forth above.

3. Defendants' Motion to Exclude Plaintiff's Expert Jay F. Freedberg [# 134] is DENIED.

4. Defendants Supplemental Motion for Sanctions [# 137] is DENIED.

5. Defendant's Motion for Summary Judgment [# 148] is DENIED.

6. The parties' Renewed Stipulated Motion to Set Dates Certain for Pre–Trial Deadlines [# 174] is GRANTED, subject to the Court's comments.

7. [Plaintiffs'] Unopposed Motion to Supplement Response to Motion to Exclude Jay E. Freedberg, CPA [# 189] is GRANTED.

D.Colo.,2013.
Christou v. Beatport, LLC
Not Reported in F.Supp.2d, 2013 WL 248058 (D.Colo.), 2013-1 Trade Cases P 78,230

END OF DOCUMENT

228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407, 164 Lab.Cas. P 61,510, 23 Wage & Hour Cas.2d (BNA) 204, 14 Cal. Daily Op. Serv. 9156, 2014 Daily Journal D.A.R. 10,735
(Cite as: 228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407)

Court of Appeal,
Second District, Division 2, California.
Colin COCHRAN, Plaintiff and Appellant,
v.
SCHWAN'S HOME SERVICE, INC., Defendant and Respondent.

B247160
Filed August 12, 2014

Background: Employee brought action against employer on behalf of customer service managers who were not reimbursed for expenses pertaining to the work-related use of their personal cell phones, alleging labor code violations and unfair business practices, and seeking declaratory relief and statutory penalties. The Superior Court, Los Angeles County, No. BC449547, Teresa Sanchez-Gordon, J., denied class certification, and employee appealed.

Holding: The Court of Appeal, Ashmann-Gerst, Acting P.J., held that employees who were required to use personal cell phones for business purposes suffered an expenditure or loss which required reimbursement.

Reversed.

West Headnotes

[1] Parties 287 35.17

287 Parties
287III Representative and Class Actions
287III(A) In General
287k35.17 k. Community of interest; commonality. Most Cited Cases

Parties 287 35.41

287 Parties
287III Representative and Class Actions
287III(B) Proceedings
287k35.41 k. Identification of class; subclasses. Most Cited Cases

A party seeking class certification must demonstrate an ascertainable class and a well-defined community of interest.

[2] Parties 287 35.13

287 Parties
287III Representative and Class Actions
287III(A) In General
287k35.13 k. Representation of class; typicality. Most Cited Cases

Parties 287 35.17

287 Parties
287III Representative and Class Actions
287III(A) In General
287k35.17 k. Community of interest; commonality. Most Cited Cases

The requisite community of interest is established in a class action when there are predominate common questions, the class representatives have claims or defenses typical of the class, and the class representatives can adequately represent the class.

[3] Parties 287 35.17

228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407, 164 Lab.Cas. P 61,510, 23 Wage & Hour Cas.2d (BNA) 204, 14 Cal. Daily Op. Serv. 9156, 2014 Daily Journal D.A.R. 10,735
(Cite as: 228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407)

287 Parties
287III Representative and Class Actions
287III(A) In General
287k35.17 k. Community of interest; commonality. Most Cited Cases

Generally, if the defendant's liability can be determined by facts common to all members of the class, a class will be certified even if the members must individually prove their damages.

[4] Parties 287 35.17

287 Parties
287III Representative and Class Actions
287III(A) In General
287k35.17 k. Community of interest; commonality. Most Cited Cases

When sufficient common questions predominate in a class action, it may be possible to manage individual issues through the use of surveys and statistical sampling.

[5] Parties 287 35.17

287 Parties
287III Representative and Class Actions
287III(A) In General
287k35.17 k. Community of interest; commonality. Most Cited Cases

Parties 287 35.33

287 Parties
287III Representative and Class Actions
287III(B) Proceedings
287k35.33 k. Evidence; pleadings and supplementary material. Most Cited Cases

Several considerations determine whether a sample is sufficiently representative in a class action to fairly support inferences about the underlying population; those considerations include variability in the population, whether size of the sample is appropriate, whether the sample is random or infected by selection bias, and whether the margin of error in the statistical analysis is reasonable.

[6] Parties 287 35.35

287 Parties
287III Representative and Class Actions
287III(B) Proceedings
287k35.35 k. Hearing and determination. Most Cited Cases

At the certification stage of a class action, a trial court considering whether individual issues can be managed should consider whether a statistical plan has been developed.

[7] Parties 287 35.9

287 Parties
287III Representative and Class Actions
287III(A) In General
287k35.9 k. Discretion of court. Most Cited Cases

Whether to grant or deny class certification is a matter within a trial court's discretion.

[8] Appeal And Error 30 854(1)

30 Appeal and Error
30XVI Review
30XVI(A) Scope, Standards, and Extent, in General
30k851 Theory and Grounds of Decision of Lower Court

228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407, 164 Lab.Cas. P 61,510, 23 Wage & Hour Cas.2d (BNA) 204, 14 Cal. Daily Op. Serv. 9156, 2014 Daily Journal D.A.R. 10,735
(Cite as: 228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407)

30k854 Reasons for Decision
30k854(1) k. In general. Most Cited Cases

Appeal And Error 30 1024.1

30 Appeal and Error
30XVI Review
30XVI(I) Questions of Fact, Verdicts, and Findings
30XVI(I)6 Questions of Fact on Motions or Other Interlocutory or Special Proceedings
30k1024.1 k. In general. Most Cited Cases

Parties 287 35.35

287 Parties
287III Representative and Class Actions
287III(B) Proceedings
287k35.35 k. Hearing and determination. Most Cited Cases

Appellate review of orders denying class certification differs from ordinary appellate review; under ordinary appellate review, the appellate court does not address the trial court's reasoning and considers only whether the result was correct, but when denying class certification, the trial court must state its reasons, and the appellate court must review those reasons for correctness.

[9] Appeal And Error 30 854(1)

30 Appeal and Error
30XVI Review
30XVI(A) Scope, Standards, and Extent, in General
30k851 Theory and Grounds of Decision of Lower Court
30k854 Reasons for Decision
30k854(1) k. In general. Most Cited Cases

The Court of Appeal considering the denial of class certification may only consider the reasons stated by the trial court and must ignore any unexpressed reason that might support the ruling.

[10] Appeal And Error 30 1024.1

30 Appeal and Error
30XVI Review
30XVI(I) Questions of Fact, Verdicts, and Findings
30XVI(I)6 Questions of Fact on Motions or Other Interlocutory or Special Proceedings
30k1024.1 k. In general. Most Cited Cases

The Court of Appeal will affirm an order denying class certification if any of the trial court's stated reasons was valid and sufficient to justify the order, and it is supported by substantial evidence.

[11] Appeal And Error 30 1024.1

30 Appeal and Error
30XVI Review
30XVI(I) Questions of Fact, Verdicts, and Findings
30XVI(I)6 Questions of Fact on Motions or Other Interlocutory or Special Proceedings
30k1024.1 k. In general. Most Cited Cases

The Court of Appeal will reverse an order denying class certification if the trial court used improper criteria or made erroneous legal assumptions, even if substantial evidence supported the order.

[12] Appeal And Error 30 946

228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407, 164 Lab.Cas. P 61,510, 23 Wage & Hour Cas.2d (BNA) 204, 14 Cal. Daily Op. Serv. 9156, 2014 Daily Journal D.A.R. 10,735
(Cite as: 228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407)

30 Appeal and Error
30XVI Review
30XVI(H) Discretion of Lower Court
30k944 Power to Review
30k946 k. Abuse of discretion. Most Cited Cases

A trial court's decision that rests on an error of law is an abuse of discretion.

[13] Labor And Employment 231H 195

231H Labor and Employment
231HIV Compensation and Benefits
231HIV(A) In General
231Hk195 k. Defending claims against employee; indemnity. Most Cited Cases

Purpose of statute requiring an employer to indemnify an employee for all necessary expenditures or losses incurred in the discharge of his or her duties is to prevent employers from passing their operating expenses on to their employees. Cal. Lab. Code § 2802(a).

[14] Labor And Employment 231H 194

231H Labor and Employment
231HIV Compensation and Benefits
231HIV(A) In General
231Hk194 k. Reimbursements and advances in general. Most Cited Cases

In calculating the reimbursement amount due to an employee for expenditures incurred in employment, the employer may consider not only the actual expenses that the employee incurred, but also whether each of those expenses was “necessary,” which in turn depends on the reasonableness of the employee's choices. Cal. Lab. Code § 2802(a).

[15] Labor And Employment 231H 194

231H Labor and Employment
231HIV Compensation and Benefits
231HIV(A) In General
231Hk194 k. Reimbursements and advances in general. Most Cited Cases

An employer always has to reimburse an employee for the reasonable expense of the mandatory use of a personal cell phone; the reimbursement obligation is not limited to the situation in which the employee incurred an extra expense that he or she would not have otherwise incurred absent the job. Cal. Lab. Code § 2802(a).

[16] Labor And Employment 231H 194

231H Labor and Employment
231HIV Compensation and Benefits
231HIV(A) In General
231Hk194 k. Reimbursements and advances in general. Most Cited Cases

Employees who were required to use personal cell phones for business purposes suffered an expenditure or loss which required reimbursement, even if cell phone charges were paid for by a third person, or if the employee did not purchase a different cell phone plan because of cell phone usage at work. Cal. Lab. Code § 2802(a).

[17] Labor And Employment 231H 194

231H Labor and Employment
231HIV Compensation and Benefits
231HIV(A) In General
231Hk194 k. Reimbursements and advances in general. Most Cited Cases

228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407, 164 Lab.Cas. P 61,510, 23 Wage & Hour Cas.2d (BNA) 204, 14 Cal. Daily Op. Serv. 9156, 2014 Daily Journal D.A.R. 10,735
(Cite as: 228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407)

To show liability for an employer's failure to reimburse an employee for necessary expenditures, an employee need only show that he or she was required to use a personal cell phone to make work-related calls, and he or she was not reimbursed. Cal. Lab. Code § 2802(a).
See 3 Witkin, Summary of Cal. Law (10th ed. 2005) Agency and Employment, § 122.

APPEAL from an order of the Superior Court of Los Angeles County. Teresa Sanchez-Gordon, Judge. Reversed. (Los Angeles County Super. Ct. No. BC449547)****409** Law Offices of Kevin T. Barnes, Kevin T. Barnes, Gregg Lander; Kokozian Law Firm and Bruce Z. Kokozian, for Plaintiff and Appellant.

Kutak Rock, Matthew C. Sgnilek; and Alan L. Rupe, for Defendant and Respondent.

ASHMANN-GERST, Acting P.J.

***1140** We hold that when employees must use their personal cell phones for work-related calls, Labor Code section 2802 [FN1] requires the employer to reimburse them. Whether the employees have cell phone plans with unlimited minutes or limited minutes, the reimbursement owed is a reasonable percentage of their cell phone bills. Because the trial court relied on erroneous legal assumptions about the application of section 2802, we must reverse the order denying certification to a class of 1,500 service managers in an action against Schwan's Home Service, Inc. (Home Service) seeking, inter lia, reimbursement of work-related cell phone expenses. Upon remand, the trial court shall reconsider the motion for class certification in light of our interpretation of section 2802. When reconsidering the motion, it shall apply the principles set forth in *Duran v. U.S. Bank National Assn.* (2014) 59 Cal.4th 1, 172 Cal.Rptr.3d 371, 325 P.3d 916 (*Duran*) to the degree that the class representative, Colin Cochran (Cochran), proposes to use statistical sampling evidence to establish either liability or damages. The parties shall have the opportunity to revise their papers to address the issues raised herein.

FN1. All further statutory references are to the Labor Code unless otherwise indicated.

FACTS

Cochran filed a putative class action against Home Service on behalf of customer service managers who were not reimbursed for expenses pertaining to the work-related use of their personal cell phones. He alleged causes of action for violation of section 2802; unfair business practices under Business and Professions Code section 17200 et seq; declaratory relief; and statutory penalties under section 2699, the Private Attorneys–General Act of 2004.

He moved to certify the class. Home Service filed an opposition as well as a motion to deny certification.

On October 24, 2012, the trial court held a hearing. It found that the class was ascertainable; the class was sufficiently numerous because it included 1,500 people; Cochran was a typical as well as an adequate class member; and counsel for the putative class was qualified to act as class counsel. Next, the trial court analyzed commonality. It determined that the elements of a section 2802 claim were: (1) expenditures by the customer service managers; (2) the expenditures were necessarily incurred in the discharge of their duties; (3) Home Service knew or had reason to know of the expenditures; and (4) ***1141** Home Service did not exercise due diligence to reimburse the expenditures. The trial court concluded that common questions predominated regarding issues 2, 3 and 4. As to the first issue, Home Service, argued that the expenditure element "is subject to ... individual questions because many people now have unlimited data plans for which they do not actually incur an additional expense when they use their cell phone. In order to determine whether an expense was incurred for [a class member's] business use will require an exami-

228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407, 164 Lab.Cas. P 61,510, 23 Wage & Hour Cas.2d (BNA) 204, 14 Cal. Daily Op. Serv. 9156, 2014 Daily Journal D.A.R. 10,735
(Cite as: 228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407)

nation of each class member's cell phone plan [.]" Cochran argued "that whether [a class member] actually incurred an expense when using their personal cell phone for work is an issue of ****410** damages and individualized damages do not impact the commonality analysis." In the trial court's view, Cochran "misstate[d] the elements of a failure to reimburse claim," explaining that "[t]he showing of an actionable expenditure or loss by ... class member[s] pertains to [Home Service's] liability, not to class members' damages as it is set forth in ... section 2802. If the class member[s] did not incur ... loss[es], there can be no liability." Next, the trial court noted that there was an issue regarding whether Cochran or his girlfriend paid for his phone bill, implying that whether each class member paid for his or her phone bill was an issue. Also, it found that the expenditure inquiry would involve questions about whether class members "purchased ... different cell phone plans because of their work cell phone usage." Because Cochran did not provide a means for managing these questions, the trial court ordered further briefing. It deferred ruling on whether a class action was a superior method for adjudicating the claims.

In his supplemental brief, Cochran argued that statistical evidence and representative testimony could be used to establish Home Service's liability. The brief was supported by the expert declaration of G. Michael Phillips, Ph.D., an economist and statistician. He opined that there were two methods for establishing liability as well as damages. First, he could assume damages of $2 per day, which was the amount he claimed that Home Service reimbursed putative class members in 2006–2007. Second, he could conduct a survey.

Regarding the latter method, Dr. Phillips provided a 22–question draft survey. He stated: "A survey implementation plan would proceed as follows: first, a letter would be mailed to the address of each class member, informing them that they would be called in the next few days to take part in an important survey. It would ask them to find their cellular telephone records, if possible, to assist with accurate data collection. Next, an interviewer would attempt to call each class member and administer the telephonic survey. For working numbers, up to five attempts would be made, at varying days and times, to reach each class member by phone. In the instance that an initial call reached a nonworking number, an attempt would be made to find an alternative number. The data from the survey would then be analyzed for ***1142** potential nonsampling errors through standard statistical procedures, and finally used for analysis of reported losses and expenditures by class members."

On January 31, 2013, the trial court held a second hearing. It denied class certification due to lack of commonality, and because a class action was not a superior method of litigating the claims. It noted that there was a question as to "whether the cell phone charges [Cochran] allegedly incurred were incurred and paid for by him or by his live-in girlfriend," and explained that this issue was resolved only after Cochran was examined. In addition, the trial court stated that Home Service "would be entitled to ask whether each driver purchased a different cell phone plan, because of their work cell phone usage[,]" and therefore Home Service had "demonstrated that these individual issues exist for" class members. The trial court added that statistics from a survey could not be used to prove liability, especially because there was no pattern or practice regarding the expenditures or losses of class members. It concluded: "[Cochran] has not demonstrated how the cell phone plans and method of payment exhibited by a portion of the class will accurately reflect the plans and method of payment for the entire class.... Therefore, individualized ****411** inquiries of the class members' cell phone plans and payments are necessary to determine liability. This inquiry for 1500 class members, as evidenced by the four-page 22 question survey, will overwhelm the liability determination. Therefore, common questions do not predominate[.]"

228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407, 164 Lab.Cas. P 61,510, 23 Wage & Hour Cas.2d (BNA) 204, 14 Cal. Daily Op. Serv. 9156, 2014 Daily Journal D.A.R. 10,735
(Cite as: 228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407)

This timely appeal followed.

DISCUSSION

I. Class Certification Law; Standard of Review.

[1][2][3]A party seeking class certification must demonstrate an ascertainable class and a well-defined community of interest. (*Soderstedt v. CBIZ Southern California, LLC* (2011) 197 Cal.App.4th 133, 142–143, 127 Cal.Rptr.3d 394.) The requisite community interest is established when there are predominate common questions, the class representatives have claims or defenses typical of the class, and the class representatives can adequately represent the class. (*Id.* at p. 143, 127 Cal.Rptr.3d 394.) Generally, " 'if the defendant's liability can be determined by facts common to all members of the class, a class will be certified even if the members must individually prove their damages.' [Citations.]" (*Brinker Restaurant Corp. v. Superior Court* (2012) 53 Cal.4th 1004, 1022, 139 Cal.Rptr.3d 315, 273 P.3d 513.)

[4][5][6]When sufficient common questions predominate, "it may be possible to manage individual issues through the use of surveys and statistical ***1143** sampling." (*Duran, supra*, 59 Cal.4th at p. 31, 172 Cal.Rptr.3d 371, 325 P.3d 916.) *Duran,* a case involving a wage and hour class action, explained that sampling is a "methodology based on inferential statistics and probability theory. 'The essence of the science of inferential statistics is that one may confidently draw inferences about the whole from a representative sample of the whole.' [Citation.] Whether such inferences are supportable, however, depends on how representative the sample is. '[I]nferences from the part to the whole are justified [*only*] when the sample is representative.' [Citation.] Several considerations determine whether a sample is sufficiently representative to fairly support inferences about the underlying population." (*Duran, supra*, at p. 38, 172 Cal.Rptr.3d 371, 325 P.3d 916.) Those considerations include variability in the population, whether size of the sample is appropriate, whether the sample is random or infected by selection bias, and whether the margin of error in the statistical analysis is reasonable. (*Id.* at pp. 38–46, 172 Cal.Rptr.3d 371, 325 P.3d 916.) At the certification stage, a trial court "should consider ... whether a [statistical] plan has been developed[.]" (*Id.* at p. 31, 172 Cal.Rptr.3d 371, 325 P.3d 916.) *Duran* noted that the use of statistical sampling to prove liability in overtime class actions is controversial, and explained that the use of it to prove damage is less so because "the law tolerates more uncertainty with respect to damages than to the existence of liability." (*Id.* at p. 40, 172 Cal.Rptr.3d 371, 325 P.3d 916.) The court stopped short of deciding whether sampling "should be available as a tool for proving liability in a class action." (*Ibid.*) Instead, inter alia, it warned that "when statistical methods such as sampling are appropriate, due concern for the parties' rights requires that they be employed with caution." (*Id.* at p. 41, 172 Cal.Rptr.3d 371, 325 P.3d 916.)

[7][8][9][10][11][12]Whether to grant or deny class certification is a matter within a trial court's discretion. That said, "appellate review of orders denying class certification differs from ordinary appellate review. Under ordinary appellate review, we do not address the trial court's reasoning and ****412** consider only whether the result was correct. [Citation.] But when denying class certification, the trial court must state its reasons, and we must review those reasons for correctness. [Citation.] We may only consider the reasons stated by the trial court and must ignore any unexpressed reason that might support the ruling. [Citations.] [¶] We will affirm an order denying class certification if any of the trial court's stated reasons was valid and sufficient to justify the order, and it is supported by substantial evidence. [Citations.] We will reverse an order denying class certification if the trial court used improper criteria or made erroneous legal assumptions, even if substantial evidence supported the order. [Citations.] A trial court's decision that rests on an error of law is an abuse of discretion. [Citations.]" (*Knapp v. AT & T Wireless Services, Inc.*

228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407, 164 Lab.Cas. P 61,510, 23 Wage & Hour Cas.2d (BNA) 204, 14 Cal. Daily Op. Serv. 9156, 2014 Daily Journal D.A.R. 10,735
(Cite as: 228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407)

(2011) 195 Cal.App.4th 932, 939, 124 Cal.Rptr.3d 565.)

II. Section 2802.

[13][14]Pursuant to section 2802, subdivision (a), "[a]n employer shall indemnify his or her employee for all necessary expenditures or losses incurred by ***1144** the employee in direct consequence of the discharge of his or her duties, or of his or her obedience to the directions of the employer [.]" The purpose of this statute is " 'to prevent employers from passing their operating expenses on to their employees.' " (*Gattuso v. Harte–Hanks Shoppers, Inc.* (2007) 42 Cal.4th 554, 562, 67 Cal.Rptr.3d 468, 169 P.3d 889 (*Gattuso*) [quoting legislative history from the 2000 amendment to the statute].) "In calculating the reimbursement amount due under section 2802, the employer may consider not only the actual expenses that the employee incurred, but also whether each of those expenses was 'necessary,' which in turn depends on the reasonableness of the employee's choices. [Citation.]" (*Gattuso, supra,* 42 Cal.4th at p. 568, 67 Cal.Rptr.3d 468, 169 P.3d 889.)

[15]The threshold question in this case is this: Does an employer always have to reimburse an employee for the reasonable expense of the mandatory use of a personal cell phone, or is the reimbursement obligation limited to the situation in which the employee incurred an extra expense that he or she would not have otherwise incurred absent the job? The answer is that reimbursement is always required. Otherwise, the employer would receive a windfall because it would be passing its operating expenses onto the employee. Thus, to be in compliance with section 2802, the employer must pay some reasonable percentage of the employee's cell phone bill. Because of the differences in cell phone plans and worked-related scenarios, the calculation of reimbursement must be left to the trial court and parties in each particular case.

III. The Order Denying Class Certification Must be Reversed Because the Court Made Erroneous Legal Assumptions.

[16]When ruling, the trial court assumed that an employee does not suffer an expenditure or loss under section 2802 if his or her cell phone charges were paid for by a third person, or if the employee did not purchase a different cell phone plan because of cell phone usage at work. In addition, the trial court assumed that liability could not be determined without an inquiry into the specifics of each class members' cell phone plan. As we discuss, each of these legal assumptions was erroneous.

[17]If an employee is required to make work-related calls on a personal cell phone, then he or she is incurring an expense for purposes of section 2802. It ****413** does not matter whether the phone bill is paid for by a third person, or at all. In other words, it is no concern to the employer that the employee may pass on the expense to a family member or friend, or to a carrier that has to then write off a loss. It is irrelevant whether the employee changed plans to accommodate worked-related cell phone usage. Also, the details of the employee's cell phone plan do not factor into the liability analysis. Not only ***1145** does our interpretation prevent employers from passing on operating expenses, it also prevents them from digging into the private lives of their employees to unearth how they handle their finances vis-a-vis family, friends and creditors. To show liability under section 2802, an employee need only show that he or she was required to use a personal cell phone to make work-related calls, and he or she was not reimbursed. Damages, of course, raise issues that are more complicated.

Because the trial court made erroneous legal assumptions, the denial of class certification must be reversed.

All other issues are moot.

DISPOSITION

228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407, 164 Lab.Cas. P 61,510, 23 Wage & Hour Cas.2d (BNA) 204, 14 Cal. Daily Op. Serv. 9156, 2014 Daily Journal D.A.R. 10,735
(Cite as: 228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407)

The order denying class certification is reversed. Upon remand, the trial court shall reconsider Cochran's motion. In doing so, the trial court shall heed our interpretation of section 2802 and apply the principles set forth in *Duran* regarding statistical sampling. Cochran shall have the opportunity to revise its motion, and Home Service shall have the opportunity to respond.

Cochran shall recover his costs on appeal.

We concur:
CHAVEZ, J.
FERNS, J.[FN*]

FN* Judge of the Los Angeles Superior Court, assigned by the Chief Justice pursuant to article VI, section 6 of the California Constitution.

Cal.App. 2 Dist., 2014
Cochran v. Schwan's Home Service, Inc.
228 Cal.App.4th 1137, 176 Cal.Rptr.3d 407, 164 Lab.Cas. P 61,510, 23 Wage & Hour Cas.2d (BNA) 204, 14 Cal. Daily Op. Serv. 9156, 2014 Daily Journal D.A.R. 10,735

END OF DOCUMENT

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

Supreme Court of the United States
David Leon RILEY, Petitioner
v.
CALIFORNIA.
United States, Petitioner
v.
Brima Wurie.

Nos. 13–132, 13–212.
Argued April 29, 2014.
Decided June 25, 2014.

Background: In two cases consolidated for appeal, first defendant was convicted by a jury in the Superior Court, San Diego County, Laura W. Halgren, J., of various crimes related to drive-by shooting, and he appealed based on his challenge to evidence found during police officers' warrantless search of data stored on his cell phone. The California Court of Appeal, 2013 WL 475242, affirmed. Second defendant was charged with drug- and weapon-related crimes, and the United States District Court for the District of Massachusetts, Stearns, J., 612 F.Supp.2d 104, denied his motion to suppress evidence found during warrantless search of data stored on his cell phone, and defendant appealed. The United States Court of Appeals for the First Circuit, Stahl, Circuit Judge, 728 F.3d 1, reversed. Certiorari was granted.

Holdings: The Supreme Court, Chief Justice Roberts, held that:
(1) interest in protecting officers' safety did not justify dispensing with warrant requirement for searches of cell phone data, and
(2) interest in preventing destruction of evidence did not justify dispensing with warrant requirement for searches of cell phone data.

Judgment of California Court of Appeal reversed and remanded, and judgment of First Circuit affirmed.

Justice Alito concurred in part and concurred in the judgment in separate opinion.

West Headnotes

[1] Searches and Seizures 349 23

349 Searches and Seizures
349I In General
349k23 k. Fourth Amendment and reasonableness in general. Most Cited Cases

Ultimate touchstone of the Fourth Amendment is reasonableness. U.S.C.A. Const.Amend. 4.

[2] Searches and Seizures 349 24

349 Searches and Seizures
349I In General
349k24 k. Necessity of and preference for warrant, and exceptions in general. Most Cited Cases

Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, reasonableness generally requires the obtaining of a judicial warrant, so as to ensure that the inferences to support a search are drawn by a neutral and detached magistrate, instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. U.S.C.A. Const.Amend. 4.

[3] Searches and Seizures 349 24

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

349 Searches and Seizures
349I In General
349k24 k. Necessity of and preference for warrant, and exceptions in general. Most Cited Cases

In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement. U.S.C.A. Const.Amend. 4.

[4] Arrest 35 71.1(6)

35 Arrest
35II On Criminal Charges
35k71.1 Search
35k71.1(4) Scope of Search
35k71.1(6) k. Persons and personal effects; person detained for investigation. Most Cited Cases

When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. U.S.C.A. Const.Amend. 4.

[5] Arrest 35 71.1(1)

35 Arrest
35II On Criminal Charges
35k71.1 Search
35k71.1(1) k. In general. Most Cited Cases

Authority to search a person incident to a lawful custodial arrest, while based upon the need to disarm and to discover evidence, does not depend on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect. U.S.C.A. Const.Amend. 4.

[6] Arrest 35 63.4(1)

35 Arrest
35II On Criminal Charges
35k63 Officers and Assistants, Arrest Without Warrant
35k63.4 Probable or Reasonable Cause
35k63.4(1) k. Grounds for warrantless arrest in general. Most Cited Cases

Arrest 35 71.1(2.1)

35 Arrest
35II On Criminal Charges
35k71.1 Search
35k71.1(2) Probable Cause; Offense in Officer's Presence
35k71.1(2.1) k. In general. Most Cited Cases

Custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification. U.S.C.A. Const.Amend. 4.

[7] Arrest 35 71.1(5)

35 Arrest
35II On Criminal Charges
35k71.1 Search
35k71.1(4) Scope of Search
35k71.1(5) k. Particular places or objects. Most Cited Cases

Under the search incident to arrest exception to the warrant requirement, police may search the vehicle's passenger compartment when it is reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle. U.S.C.A. Const.Amend. 4.

[8] Searches and Seizures 349 24

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

349 Searches and Seizures
349I In General
349k24 k. Necessity of and preference for warrant, and exceptions in general. Most Cited Cases

Generally, to determine whether to exempt a given type of search from the warrant requirement, courts must assess, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests. U.S.C.A. Const.Amend. 4.

[9] Arrest 35 71.1(6)

35 Arrest
35II On Criminal Charges
35k71.1 Search
35k71.1(4) Scope of Search
35k71.1(6) k. Persons and personal effects; person detained for investigation. Most Cited Cases

Under search incident to arrest exception, interest in protecting police officers' safety did not justify dispensing with warrant requirement before officers could search digital data on arrestees' cell phones; although officers remained free to examine physical aspects of phone to ensure that it could not be used as weapon, digital data stored on phones could not itself be used as weapon to harm officers or to effectuate arrestees' escape, and, to extent dangers to officers could be implicated in particular cases, those dangers could be addressed through consideration of, for example, exception for exigent circumstances. U.S.C.A. Const.Amend. 4.

[10] Arrest 35 71.1(6)

35 Arrest
35II On Criminal Charges
35k71.1 Search
35k71.1(4) Scope of Search
35k71.1(6) k. Persons and personal effects; person detained for investigation. Most Cited Cases

Under search incident to arrest exception, interest in preventing destruction of evidence did not justify dispensing with warrant requirement before officers could search digital data on arrestees' cell phones; officers expressed concerns about possibility of remote wiping of data or of encryption of data when phones “locked,” but those broad concerns were distinct from concern over arrestees concealing or destroying evidence within their reach, as these concerns involved acts by third parties or normal operation of phones' security features, officers had some technologies available to them to counteract these concerns, and remaining issues could be addressed in particular cases by responding in targeted manner to urgent threats of remote wiping or by disabling phones' locking mechanism in order to secure crime scene. U.S.C.A. Const.Amend. 4.

[11] Arrest 35 71.1(1)

35 Arrest
35II On Criminal Charges
35k71.1 Search
35k71.1(1) k. In general. Most Cited Cases

Search incident to arrest exception to the warrant requirement rests not only on the heightened government interests at stake in a volatile arrest situation, but also on the arrestee's reduced privacy interests upon being taken into police custody. U.S.C.A. Const.Amend. 4.

[12] Arrest 35 71.1(4.1)

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

35 Arrest
35II On Criminal Charges
35k71.1 Search
35k71.1(4) Scope of Search
35k71.1(4.1) k. In general. Most Cited Cases

Not every search is acceptable solely because a person is in custody; to the contrary, when privacy-related concerns are weighty enough, a search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee. U.S.C.A. Const.Amend. 4.

[13] Arrest 35 71.1(6)

35 Arrest
35II On Criminal Charges
35k71.1 Search
35k71.1(4) Scope of Search
35k71.1(6) k. Persons and personal effects; person detained for investigation. Most Cited Cases

Under search incident to arrest exception, privacy concerns with data stored on arrestees' cell phones dwarfed those involved with physical objects, and thus extending conclusion that inspection of physical objects worked no substantial additional intrusion on privacy beyond arrest itself to include police officers' search of cell phone data was unwarranted; cell phones differed from other physical objects both quantitatively and qualitatively, given phones' immense storage capacity, collection in one place of many distinct types of private information, and ability to convey more information than previously possible, and phones also presented issue that they can access information not stored on phones themselves, which information government conceded was not covered by this exception. U.S.C.A. Const.Amend. 4.

[14] Arrest 35 71.1(6)

35 Arrest
35II On Criminal Charges
35k71.1 Search
35k71.1(4) Scope of Search
35k71.1(6) k. Persons and personal effects; person detained for investigation. Most Cited Cases

Extending standard of *Arizona v. Gant*, which allowed warrantless searches in vehicle context whenever police officers had reasonable belief that vehicle contained evidence of crime of arrest, to officers' search of digital data stored on arrestees' cell phones was unwarranted under search incident to arrest exception to warrant requirement; *Gant* relied on circumstances unique to vehicle context, specifically reduced expectation of privacy and heightened law enforcement needs, but cell phone searches bore neither of those concerns, and *Gant* standard, which generally protected against searches for evidence of past crimes and restricted broad searches resulting from minor crimes, would provide no practical limit on cell phone searches, given broad, historical information stored on phones. U.S.C.A. Const.Amend. 4.

[15] Arrest 35 71.1(6)

35 Arrest
35II On Criminal Charges
35k71.1 Search
35k71.1(4) Scope of Search
35k71.1(6) k. Persons and personal effects; person detained for investigation. Most Cited Cases

Under search incident to arrest exception to warrant requirement, proposed rule restricting scope of police officers' warrantless searches of cell phones to those areas of phone in which officers reasonably believed that information relevant to crime of arrest, arrestee's identity, or officer safety would be discov-

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

ered would impose no meaningful constraints on officers, since those categories would sweep in great deal of information, and officers would not always be able to discern in advance what information would be found where. U.S.C.A. Const.Amend. 4.

[16] Arrest 35 71.1(6)

35 Arrest
35II On Criminal Charges
35k71.1 Search
35k71.1(4) Scope of Search
35k71.1(6) k. Persons and personal effects; person detained for investigation. Most Cited Cases

Proposed rule permitting police officers to conduct warrantless searches of call logs on arrestees' cell phones was unwarranted under search incident to arrest exception to warrant requirement, since those logs would typically contain not only phone numbers, but also identifying information that arrestee might have added, such as labels for incoming calls. U.S.C.A. Const.Amend. 4.

[17] Arrest 35 71.1(6)

35 Arrest
35II On Criminal Charges
35k71.1 Search
35k71.1(4) Scope of Search
35k71.1(6) k. Persons and personal effects; person detained for investigation. Most Cited Cases

Proposed rule permitting police officers to conduct warrantless search of arrestees' cell phone data if they could have obtained same information from pre-digital counterpart was unwarranted under search incident to arrest exception to warrant requirement; fact that pre-digital search could have turned up a few photographs in arrestee's wallet or paper bank statement kept in pocket did not justify search of potentially thousands of photographs and extensive bank records, rule would permit officers to search range of information contained on cell phone, even though people would be unlikely to carry such information in physical form, and rule would force courts to engage in complex line-drawing exercise to determine digital to pre-digital analogues. U.S.C.A. Const.Amend. 4.

[18] Searches and Seizures 349 42.1

349 Searches and Seizures
349I In General
349k42 Emergencies and Exigent Circumstances; Opportunity to Obtain Warrant
349k42.1 k. In general. Most Cited Cases

Exigent circumstances exception to the warrant requirement applies when the exigencies of the situation, such as the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury, make the needs of law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment. U.S.C.A. Const.Amend. 4.

[19] Arrest 35 71.1(1)

35 Arrest
35II On Criminal Charges
35k71.1 Search
35k71.1(1) k. In general. Most Cited Cases

Searches and Seizures 349 42.1

349 Searches and Seizures
349I In General
349k42 Emergencies and Exigent Circumstances; Opportunity to Obtain Warrant

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

349k42.1 k. In general. Most Cited Cases

Unlike the search incident to arrest exception to the warrant requirement, the exigent circumstances exception requires a court to examine whether an emergency justified a warrantless search in each particular case. U.S.C.A. Const.Amend. 4.

***2477** *Syllabus* [FN*]

FN* The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States v. Detroit Timber & Lumber Co.*, 200 U.S. 321, 337, 26 S.Ct. 282, 50 L.Ed. 499.

In No. 13–132, petitioner Riley was stopped for a traffic violation, which eventually led to his arrest on weapons charges. An officer searching Riley incident to the arrest seized a cell phone from Riley's pants pocket. The officer accessed information on the phone and noticed the repeated use of a term associated with a street gang. At the police station two hours later, a detective specializing in gangs further examined the phone's digital contents. Based in part on photographs and videos that the detective found, the State charged Riley in connection with a shooting that had occurred a few weeks earlier and sought an enhanced sentence based on Riley's gang membership. Riley moved to suppress all evidence that the police had obtained from his cell phone. The trial court denied the motion, and Riley was convicted. The California Court of Appeal affirmed.

In No. 13–212, respondent Wurie was arrested after police observed him participate in an apparent drug sale. At the police station, the officers seized a cell phone from Wurie's person and noticed that the phone was receiving multiple calls from a source identified as "my house" on its external screen. The officers opened the phone, accessed its call log, determined the number associated with the "my house" label, and traced that number to what they suspected was Wurie's apartment. They secured a search warrant and found drugs, a firearm and ammunition, and cash in the ensuing search. Wurie was then charged with drug and firearm offenses. He moved to suppress the evidence obtained from the search of the apartment. The District Court denied the motion, and Wurie was convicted. The First Circuit reversed the denial of the motion to suppress and vacated the relevant convictions.

Held : The police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested. Pp. 2482 – 2495.

(a) A warrantless search is reasonable only if it falls within a specific exception to the Fourth Amendment's warrant requirement. See *Kentucky v. King*, 563 U.S. ——, ——, 131 S.Ct. 1849, 179 L.Ed.2d 865. The well-established exception at issue here applies when a warrantless search is conducted incident to a lawful arrest.

Three related precedents govern the extent to which officers may search property found on or near an arrestee. *Chimel v. California*, 395 U.S. 752, 89 S.Ct. 2034, 23 L.Ed.2d 685, requires that a search incident to arrest be limited to the area within the arrestee's immediate control, where it is justified by the interests in officer safety and in preventing evidence destruction. In *United States v. Robinson*, 414 U.S. 218, 94 S.Ct. 467, 38 L.Ed.2d 427, the Court applied the *Chimel* analysis to a search of a cigarette pack found on the arrestee's person. It held that the risks identified in *Chimel* are present in all custodial arrests, 414 U.S., at 235, 94 S.Ct. 494, even when there is no specific concern about the loss of evidence or the threat to officers in a particular case, *id.*, at 236, 94 S.Ct. 494. The trilogy concludes with *Arizona v. Gant*, 556 U.S. 332, 129 S.Ct. 1710, 173 L.Ed.2d 485,

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

which permits searches of a car where the arrestee is unsecured and within reaching distance of the passenger compartment, or where it is reasonable to believe that evidence of the crime of ***2478** arrest might be found in the vehicle, *id.*, at 343, 94 S.Ct. 494. Pp. 2482 – 2484.

(b) The Court declines to extend *Robinson* 's categorical rule to searches of data stored on cell phones. Absent more precise guidance from the founding era, the Court generally determines whether to exempt a given type of search from the warrant requirement "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Wyoming v. Houghton,* 526 U.S. 295, 300, 119 S.Ct. 1297, 143 L.Ed.2d 408. That balance of interests supported the search incident to arrest exception in *Robinson.* But a search of digital information on a cell phone does not further the government interests identified in *Chimel,* and implicates substantially greater individual privacy interests than a brief physical search. Pp. 2484 – 2491.

(1) The digital data stored on cell phones does not present either *Chimel* risk. Pp. 2485 – 2488.

(i) Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Officers may examine the phone's physical aspects to ensure that it will not be used as a weapon, but the data on the phone can endanger no one. To the extent that a search of cell phone data might warn officers of an impending danger, *e.g.*, that the arrestee's confederates are headed to the scene, such a concern is better addressed through consideration of case-specific exceptions to the warrant requirement, such as exigent circumstances. See, *e.g.*, *Warden, Md. Penitentiary v. Hayden,* 387 U.S. 294, 298–299, 87 S.Ct. 1642, 18 L.Ed.2d 782. Pp. 2485 – 2486.

(ii) The United States and California raise concerns about the destruction of evidence, arguing that, even if the cell phone is physically secure, information on the cell phone remains vulnerable to remote wiping and data encryption. As an initial matter, those broad concerns are distinct from *Chimel* 's focus on a defendant who responds to arrest by trying to conceal or destroy evidence within his reach. The briefing also gives little indication that either problem is prevalent or that the opportunity to perform a search incident to arrest would be an effective solution. And, at least as to remote wiping, law enforcement currently has some technologies of its own for combatting the loss of evidence. Finally, law enforcement's remaining concerns in a particular case might be addressed by responding in a targeted manner to urgent threats of remote wiping, see *Missouri v. McNeely,* 569 U.S. ——, ——, 133 S.Ct. 1552, 185 L.Ed.2d 696, or by taking action to disable a phone's locking mechanism in order to secure the scene, see *Illinois v. McArthur,* 531 U.S. 326, 331–333, 121 S.Ct. 946, 148 L.Ed.2d 838. Pp. 2486 – 2488.

(2) A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but more substantial privacy interests are at stake when digital data is involved. Pp. 2488 – 2491.

(i) Cell phones differ in both a quantitative and a qualitative sense from other objects that might be carried on an arrestee's person. Notably, modern cell phones have an immense storage capacity. Before cell phones, a search of a person was limited by physical realities and generally constituted only a narrow intrusion on privacy. But cell phones can store millions of pages of text, thousands of pictures, or hundreds of videos. This has several interrelated privacy consequences. First, a ***2479** cell phone collects in one place many distinct types of information that reveal much more in combination than any isolated record. Second,

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

the phone's capacity allows even just one type of information to convey far more than previously possible. Third, data on the phone can date back for years. In addition, an element of pervasiveness characterizes cell phones but not physical records. A decade ago officers might have occasionally stumbled across a highly personal item such as a diary, but today many of the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives. Pp. 2489 – 2491.

(ii) The scope of the privacy interests at stake is further complicated by the fact that the data viewed on many modern cell phones may in fact be stored on a remote server. Thus, a search may extend well beyond papers and effects in the physical proximity of an arrestee, a concern that the United States recognizes but cannot definitively foreclose. P. 2491.

(c) Fallback options offered by the United States and California are flawed and contravene this Court's general preference to provide clear guidance to law enforcement through categorical rules. See *Michigan v. Summers*, 452 U.S. 692, 705, n. 19, 101 S.Ct. 2587, 69 L.Ed.2d 340. One possible rule is to import the *Gant* standard from the vehicle context and allow a warrantless search of an arrestee's cell phone whenever it is reasonable to believe that the phone contains evidence of the crime of arrest. That proposal is not appropriate in this context, and would prove no practical limit at all when it comes to cell phone searches. Another possible rule is to restrict the scope of a cell phone search to information relevant to the crime, the arrestee's identity, or officer safety. That proposal would again impose few meaningful constraints on officers. Finally, California suggests an analogue rule, under which officers could search cell phone data if they could have obtained the same information from a pre-digital counterpart. That proposal would allow law enforcement to search a broad range of items contained on a phone even though people would be unlikely to carry such a variety of information in physical form, and would launch courts on a difficult line-drawing expedition to determine which digital files are comparable to physical records. Pp. 2491 – 2493.

(d) It is true that this decision will have some impact on the ability of law enforcement to combat crime. But the Court's holding is not that the information on a cell phone is immune from search; it is that a warrant is generally required before a search. The warrant requirement is an important component of the Court's Fourth Amendment jurisprudence, and warrants may be obtained with increasing efficiency. In addition, although the search incident to arrest exception does not apply to cell phones, the continued availability of the exigent circumstances exception may give law enforcement a justification for a warrantless search in particular cases. Pp. 2493 – 2494.

No. 13–132, reversed and remanded; No. 13–212, 728 F.3d 1, affirmed.

ROBERTS, C.J., delivered the opinion of the Court, in which SCALIA, KENNEDY, THOMAS, GINSBURG, BREYER, SOTOMAYOR, and KAGAN, JJ., joined. ALITO, J., filed an opinion concurring in part and concurring in the judgment.
Jeffrey L. Fisher, Stanford, CA, for Petitioner Riley.

Edward C. Dumont, San Diego, CA, for Respondent California.

***2480** Michael R. Dreeben, for the United States as amicus curiae, by special leave of the Court, supporting the Respondent.

Patrick Morgan Ford, Law Office of Patrick Morgan Ford, San Diego, CA, Donald B. Ayer, Jones Day, Washington, DC, Jeffrey L. Fisher, Counsel of Record, Stanford Law School, Supreme Court Litigation Clinic, Stanford, CA, for Petitioner Riley.

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

Kamala D. Harris, Attorney General of California, Edward C. Dumont, Solicitor General, Dane R. Gillette, Chief Assistant Attorney General, Julie L. Garland, Senior Assistant Attorney General, Steven T. Oetting, Craig J. Konnoth, Deputy Solicitors General, Christine M. Levingston Bergman, Counsel of Record, Deputy Attorney General, State of California Department of Justice, San Diego, CA, for Respondent California.

Donald B. Verrilli, Jr., Solicitor General, Counsel of Record, Department of Justice, Washington, DC, for the United States.

Judith H. Mizner, Counsel of Record, Federal Defender Office, for Respondent Wurie.

Donald B. Verrilli, Jr., Solicitor General, Counsel of Record, Mythili Raman, Acting Assistant Attorney General, Michael R. Dreeben, Deputy Solicitor General, John F. Bash, Assistant to the Solicitor General, Robert A. Parker, Michael A. Rotker, Attorneys, Department of Justice, Washington, DC, for the United States.

For U.S. Supreme Court briefs, see:2014 WL 1616435 (Reply.Brief)2014 WL 1348466 (Resp.Brief)2014 WL 844599 (Pet.Brief)2014 WL 1616437 (Reply.Brief)2014 WL 1348467 (Resp.Brief)2014 WL 828012 (Pet.Brief)

Chief Justice ROBERTS delivered the opinion of the Court.

These two cases raise a common question: whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.

I

A

In the first case, petitioner David Riley was stopped by a police officer for driving with expired registration tags. In the course of the stop, the officer also learned that Riley's license had been suspended. The officer impounded Riley's car, pursuant to department policy, and another officer conducted an inventory search of the car. Riley was arrested for possession of concealed and loaded firearms when that search turned up two handguns under the car's hood. See Cal.Penal Code Ann. §§ 12025(a)(1), 12031(a)(1) (West 2009).

An officer searched Riley incident to the arrest and found items associated with the "Bloods" street gang. He also seized a cell phone from Riley's pants pocket. According to Riley's uncontradicted assertion, the phone was a "smart phone," a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity. The officer accessed information on the phone and noticed that some words (presumably in text messages or a contacts list) were preceded by the letters "CK"—a label that, he believed, stood for "Crip Killers," a slang term for members of the Bloods gang.

At the police station about two hours after the arrest, a detective specializing in gangs further examined the contents of the phone. The detective testified that he "went through" Riley's phone "looking for evidence, because ... gang members will ***2481** often video themselves with guns or take pictures of themselves with the guns." App. in No. 13–132, p. 20. Although there was "a lot of stuff" on the phone, particular files that "caught [the detective's] eye" included videos of young men sparring while someone yelled encouragement using the moniker "Blood." *Id.*, at 11–13. The police also found photographs of Riley standing in front of a car they suspected had been involved in a shooting a few weeks earlier.

Riley was ultimately charged, in connection with

that earlier shooting, with firing at an occupied vehicle, assault with a semiautomatic firearm, and attempted murder. The State alleged that Riley had committed those crimes for the benefit of a criminal street gang, an aggravating factor that carries an enhanced sentence. Compare Cal.Penal Code Ann. § 246 (2008) with § 186.22(b)(4)(B) (2014). Prior to trial, Riley moved to suppress all evidence that the police had obtained from his cell phone. He contended that the searches of his phone violated the Fourth Amendment, because they had been performed without a warrant and were not otherwise justified by exigent circumstances. The trial court rejected that argument. App. in No. 13–132, at 24, 26. At Riley's trial, police officers testified about the photographs and videos found on the phone, and some of the photographs were admitted into evidence. Riley was convicted on all three counts and received an enhanced sentence of 15 years to life in prison.

The California Court of Appeal affirmed. No. D059840 (Cal. App., Feb. 8, 2013), App. to Pet. for Cert. in No. 13–132, pp. 1a–23a. The court relied on the California Supreme Court's decision in *People v. Diaz*, 51 Cal.4th 84, 119 Cal.Rptr.3d 105, 244 P.3d 501 (2011), which held that the Fourth Amendment permits a warrantless search of cell phone data incident to an arrest, so long as the cell phone was immediately associated with the arrestee's person. See *id.*, at 93, 119 Cal.Rptr.3d 105, 244 P.3d, at 505–506.

The California Supreme Court denied Riley's petition for review, App. to Pet. for Cert. in No. 13–132, at 24a, and we granted certiorari, 571 U.S. ——, 132 S.Ct. 94, 181 L.Ed.2d 23 (2014).

B

In the second case, a police officer performing routine surveillance observed respondent Brima Wurie make an apparent drug sale from a car. Officers subsequently arrested Wurie and took him to the police station. At the station, the officers seized two cell phones from Wurie's person. The one at issue here was a "flip phone," a kind of phone that is flipped open for use and that generally has a smaller range of features than a smart phone. Five to ten minutes after arriving at the station, the officers noticed that the phone was repeatedly receiving calls from a source identified as "my house" on the phone's external screen. A few minutes later, they opened the phone and saw a photograph of a woman and a baby set as the phone's wallpaper. They pressed one button on the phone to access its call log, then another button to determine the phone number associated with the "my house" label. They next used an online phone directory to trace that phone number to an apartment building.

When the officers went to the building, they saw Wurie's name on a mailbox and observed through a window a woman who resembled the woman in the photograph on Wurie's phone. They secured the apartment while obtaining a search warrant and, upon later executing the warrant, found and seized 215 grams of crack cocaine, marijuana, drug paraphernalia, a firearm and ammunition, and cash.

***2482** Wurie was charged with distributing crack cocaine, possessing crack cocaine with intent to distribute, and being a felon in possession of a firearm and ammunition. See 18 U.S.C. § 922(g); 21 U.S.C. § 841(a). He moved to suppress the evidence obtained from the search of the apartment, arguing that it was the fruit of an unconstitutional search of his cell phone. The District Court denied the motion. 612 F.Supp.2d 104 (Mass.2009). Wurie was convicted on all three counts and sentenced to 262 months in prison.

A divided panel of the First Circuit reversed the denial of Wurie's motion to suppress and vacated Wurie's convictions for possession with intent to distribute and possession of a firearm as a felon. 728 F.3d 1 (2013). The court held that cell phones are distinct from other physical possessions that may be searched incident to arrest without a warrant, because of the

amount of personal data cell phones contain and the negligible threat they pose to law enforcement interests. See *id.*, at 8–11.

We granted certiorari. 571 U.S. ——, 134 S.Ct. 999, 187 L.Ed.2d 848 (2014).

II

The Fourth Amendment provides:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[1][2][3] As the text makes clear, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.' " *Brigham City v. Stuart*, 547 U.S. 398, 403, 126 S.Ct. 1943, 164 L.Ed.2d 650 (2006). Our cases have determined that "[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, ... reasonableness generally requires the obtaining of a judicial warrant." *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653, 115 S.Ct. 2386, 132 L.Ed.2d 564 (1995). Such a warrant ensures that the inferences to support a search are "drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime." *Johnson v. United States*, 333 U.S. 10, 14, 68 S.Ct. 367, 92 L.Ed. 436 (1948). In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement. See *Kentucky v. King*, 563 U.S. ——, ——, 131 S.Ct. 1849, 1856–1857, 179 L.Ed.2d 865 (2011).

The two cases before us concern the reasonableness of a warrantless search incident to a lawful arrest. In 1914, this Court first acknowledged in dictum "the right on the part of the Government, always recognized under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime." *Weeks v. United States*, 232 U.S. 383, 392, 34 S.Ct. 341, 58 L.Ed. 652. Since that time, it has been well accepted that such a search constitutes an exception to the warrant requirement. Indeed, the label "exception" is something of a misnomer in this context, as warrantless searches incident to arrest occur with far greater frequency than searches conducted pursuant to a warrant. See 3 W. LaFave, Search and Seizure § 5.2(b), p. 132, and n. 15 (5th ed. 2012).

Although the existence of the exception for such searches has been recognized for a century, its scope has been debated for nearly as long. See ***2483** *Arizona v. Gant*, 556 U.S. 332, 350, 129 S.Ct. 1710, 173 L.Ed.2d 485 (2009) (noting the exception's "checkered history"). That debate has focused on the extent to which officers may search property found on or near the arrestee. Three related precedents set forth the rules governing such searches:

The first, *Chimel v. California*, 395 U.S. 752, 89 S.Ct. 2034, 23 L.Ed.2d 685 (1969), laid the groundwork for most of the existing search incident to arrest doctrine. Police officers in that case arrested Chimel inside his home and proceeded to search his entire three-bedroom house, including the attic and garage. In particular rooms, they also looked through the contents of drawers. *Id.*, at 753–754, 89 S.Ct. 2034.

[4] The Court crafted the following rule for assessing the reasonableness of a search incident to arrest:

> "When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

> endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction.... There is ample justification, therefore, for a search of the arrestee's person and the area 'within his immediate control'—construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence." *Id.*, at 762–763, 89 S.Ct. 2034.

The extensive warrantless search of Chimel's home did not fit within this exception, because it was not needed to protect officer safety or to preserve evidence. *Id.*, at 763, 768, 89 S.Ct. 2034.

Four years later, in *United States v. Robinson*, 414 U.S. 218, 94 S.Ct. 467, 38 L.Ed.2d 427 (1973), the Court applied the *Chimel* analysis in the context of a search of the arrestee's person. A police officer had arrested Robinson for driving with a revoked license. The officer conducted a patdown search and felt an object that he could not identify in Robinson's coat pocket. He removed the object, which turned out to be a crumpled cigarette package, and opened it. Inside were 14 capsules of heroin. *Id.*, at 220, 223, 89 S.Ct. 2034.

[5][6] The Court of Appeals concluded that the search was unreasonable because Robinson was unlikely to have evidence of the crime of arrest on his person, and because it believed that extracting the cigarette package and opening it could not be justified as part of a protective search for weapons. This Court reversed, rejecting the notion that "case-by-case adjudication" was required to determine "whether or not there was present one of the reasons supporting the authority for a search of the person incident to a lawful arrest." *Id.*, at 235, 89 S.Ct. 2034. As the Court explained, "[t]he authority to search the person incident to a lawful custodial arrest, while based upon the need to disarm and to discover evidence, does not depend on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect." *Ibid.* Instead, a "custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification." *Ibid.*

The Court thus concluded that the search of Robinson was reasonable even though there was no concern about the loss of evidence, and the arresting officer had no specific concern that Robinson might be armed. *Id.*, at 236, 89 S.Ct. 2034. ***2484** In doing so, the Court did not draw a line between a search of Robinson's person and a further examination of the cigarette pack found during that search. It merely noted that, "[h]aving in the course of a lawful search come upon the crumpled package of cigarettes, [the officer] was entitled to inspect it." *Ibid.* A few years later, the Court clarified that this exception was limited to "personal property ... immediately associated with the person of the arrestee." *United States v. Chadwick*, 433 U.S. 1, 15, 97 S.Ct. 2476, 53 L.Ed.2d 538 (1977) (200–pound, locked footlocker could not be searched incident to arrest), abrogated on other grounds by *California v. Acevedo*, 500 U.S. 565, 111 S.Ct. 1982, 114 L.Ed.2d 619 (1991).

[7] The search incident to arrest trilogy concludes with *Gant*, which analyzed searches of an arrestee's vehicle. *Gant*, like *Robinson*, recognized that the *Chimel* concerns for officer safety and evidence preservation underlie the search incident to arrest exception. See 556 U.S., at 338, 129 S.Ct. 1710. As a result, the Court concluded that *Chimel* could authorize police to search a vehicle "only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search." 556 U.S., at 343, 129 S.Ct. 1710. *Gant* added, however, an independent exception for a warrantless search of a vehicle's passenger compartment "when it is 'rea-

sonable to believe evidence relevant to the crime of arrest might be found in the vehicle.' " *Ibid.* (quoting *Thornton v. United States*, 541 U.S. 615, 632, 124 S.Ct. 2127, 158 L.Ed.2d 905 (2004) (SCALIA, J., concurring in judgment)). That exception stems not from *Chimel*, the Court explained, but from "circumstances unique to the vehicle context." 556 U.S., at 343, 129 S.Ct. 1710.

III

These cases require us to decide how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy. A smart phone of the sort taken from Riley was unheard of ten years ago; a significant majority of American adults now own such phones. See A. Smith, Pew Research Center, Smartphone Ownership—2013 Update (June 5, 2013). Even less sophisticated phones like Wurie's, which have already faded in popularity since Wurie was arrested in 2007, have been around for less than 15 years. Both phones are based on technology nearly inconceivable just a few decades ago, when *Chimel* and *Robinson* were decided.

[8] Absent more precise guidance from the founding era, we generally determine whether to exempt a given type of search from the warrant requirement "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Wyoming v. Houghton*, 526 U.S. 295, 300, 119 S.Ct. 1297, 143 L.Ed.2d 408 (1999). Such a balancing of interests supported the search incident to arrest exception in *Robinson*, and a mechanical application of *Robinson* might well support the warrantless searches at issue here.

But while *Robinson* 's categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones. On the government interest side, *Robinson* concluded that the two risks identified in *Chimel*—harm to officers and destruction of evidence—are present in all custodial ***2485** arrests. There are no comparable risks when the search is of digital data. In addition, *Robinson* regarded any privacy interests retained by an individual after arrest as significantly diminished by the fact of the arrest itself. Cell phones, however, place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson.*

We therefore decline to extend *Robinson* to searches of data on cell phones, and hold instead that officers must generally secure a warrant before conducting such a search.

A

We first consider each *Chimel* concern in turn. In doing so, we do not overlook *Robinson* 's admonition that searches of a person incident to arrest, "while based upon the need to disarm and to discover evidence," are reasonable regardless of "the probability in a particular arrest situation that weapons or evidence would in fact be found." 414 U.S., at 235, 94 S.Ct. 467. Rather than requiring the "case-by-case adjudication" that *Robinson* rejected, *ibid.*, we ask instead whether application of the search incident to arrest doctrine to this particular category of effects would "untether the rule from the justifications underlying the *Chimel* exception," *Gant*, *supra*, at 343, 129 S.Ct. 1710. See also *Knowles v. Iowa*, 525 U.S. 113, 119, 119 S.Ct. 484, 142 L.Ed.2d 492 (1998) (declining to extend *Robinson* to the issuance of citations, "a situation where the concern for officer safety is not present to the same extent and the concern for destruction or loss of evidence is not present at all").

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

1

[9] Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade hidden between the phone and its case. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one.

Perhaps the same might have been said of the cigarette pack seized from Robinson's pocket. Once an officer gained control of the pack, it was unlikely that Robinson could have accessed the pack's contents. But unknown physical objects may always pose risks, no matter how slight, during the tense atmosphere of a custodial arrest. The officer in *Robinson* testified that he could not identify the objects in the cigarette pack but knew they were not cigarettes. See 414 U.S., at 223, 236, n. 7, 94 S.Ct. 467. Given that, a further search was a reasonable protective measure. No such unknowns exist with respect to digital data. As the First Circuit explained, the officers who searched Wurie's cell phone "knew exactly what they would find therein: data. They also knew that the data could not harm them." 728 F.3d, at 10.

The United States and California both suggest that a search of cell phone data might help ensure officer safety in more indirect ways, for example by alerting officers that confederates of the arrestee are headed to the scene. There is undoubtedly a strong government interest in warning officers about such possibilities, but neither the United States nor California offers evidence to suggest that their concerns are based on actual experience. The ***2486** proposed consideration would also represent a broadening of *Chimel*'s concern that an *arrestee himself* might grab a weapon and use it against an officer "to resist arrest or effect his escape." 395 U.S., at 763, 89 S.Ct. 2034. And any such threats from outside the arrest scene do not "lurk[ ] in all custodial arrests." *Chadwick*, 433 U.S., at 14–15, 97 S.Ct. 2476. Accordingly, the interest in protecting officer safety does not justify dispensing with the warrant requirement across the board. To the extent dangers to arresting officers may be implicated in a particular way in a particular case, they are better addressed through consideration of case-specific exceptions to the warrant requirement, such as the one for exigent circumstances. See, *e.g.*, *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 298–299, 87 S.Ct. 1642, 18 L.Ed.2d 782 (1967)("The Fourth Amendment does not require police officers to delay in the course of an investigation if to do so would gravely endanger their lives or the lives of others.").

2

The United States and California focus primarily on the second *Chimel* rationale: preventing the destruction of evidence.

[10] Both Riley and Wurie concede that officers could have seized and secured their cell phones to prevent destruction of evidence while seeking a warrant. See Brief for Petitioner in No. 13–132, p. 20; Brief for Respondent in No. 13–212, p. 41. That is a sensible concession. See *Illinois v. McArthur*, 531 U.S. 326, 331–333, 121 S.Ct. 946, 148 L.Ed.2d 838 (2001); *Chadwick*, *supra*, at 13, and n. 8, 97 S.Ct. 2476. And once law enforcement officers have secured a cell phone, there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone.

The United States and California argue that information on a cell phone may nevertheless be vulnerable to two types of evidence destruction unique to digital data—remote wiping and data encryption. Remote wiping occurs when a phone, connected to a wireless network, receives a signal that erases stored data. This can happen when a third party sends a re-

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921

mote signal or when a phone is preprogrammed to delete data upon entering or leaving certain geographic areas (so-called "geofencing"). See Dept. of Commerce, National Institute of Standards and Technology, R. Ayers, S. Brothers, & W. Jansen, Guidelines on Mobile Device Forensics (Draft) 29, 31 (SP 800–101 Rev. 1, Sept. 2013) (hereinafter Ayers). Encryption is a security feature that some modern cell phones use in addition to password protection. When such phones lock, data becomes protected by sophisticated encryption that renders a phone all but "unbreakable" unless police know the password. Brief for United States as *Amicus Curiae* in No. 13–132, p. 11.

As an initial matter, these broader concerns about the loss of evidence are distinct from *Chimel* 's focus on a defendant who responds to arrest by trying to conceal or destroy evidence within his reach. See 395 U.S., at 763–764, 89 S.Ct. 2034. With respect to remote wiping, the Government's primary concern turns on the actions of third parties who are not present at the scene of arrest. And data encryption is even further afield. There, the Government focuses on the ordinary operation of a phone's security features, apart from *any* active attempt by a defendant or his associates to conceal or destroy evidence upon arrest.

We have also been given little reason to believe that either problem is prevalent. The briefing reveals only a couple of anecdotal examples of remote wiping triggered by an arrest. See Brief for Association of State Criminal Investigative Agencies et ***2487** al. as *Amici Curiae* in No. 13–132, pp. 9–10; see also Tr. of Oral Arg. in No. 13–132, p. 48. Similarly, the opportunities for officers to search a password-protected phone before data becomes encrypted are quite limited. Law enforcement officers are very unlikely to come upon such a phone in an unlocked state because most phones lock at the touch of a button or, as a default, after some very short period of inactivity. See, *e.g.*, iPhone User Guide for iOS 7.1 Software 10 (2014) (default lock after about one minute). This may explain why the encryption argument was not made until the merits stage in this Court, and has never been considered by the Courts of Appeals.

Moreover, in situations in which an arrest might trigger a remote-wipe attempt or an officer discovers an unlocked phone, it is not clear that the ability to conduct a warrantless search would make much of a difference. The need to effect the arrest, secure the scene, and tend to other pressing matters means that law enforcement officers may well not be able to turn their attention to a cell phone right away. See Tr. of Oral Arg. in No. 13–132, at 50; see also Brief for United States as *Amicus Curiae* in No. 13–132, at 19. Cell phone data would be vulnerable to remote wiping from the time an individual anticipates arrest to the time any eventual search of the phone is completed, which might be at the station house hours later. Likewise, an officer who seizes a phone in an unlocked state might not be able to begin his search in the short time remaining before the phone locks and data becomes encrypted.

In any event, as to remote wiping, law enforcement is not without specific means to address the threat. Remote wiping can be fully prevented by disconnecting a phone from the network. There are at least two simple ways to do this: First, law enforcement officers can turn the phone off or remove its battery. Second, if they are concerned about encryption or other potential problems, they can leave a phone powered on and place it in an enclosure that isolates the phone from radio waves. See Ayers 30–31. Such devices are commonly called "Faraday bags," after the English scientist Michael Faraday. They are essentially sandwich bags made of aluminum foil: cheap, lightweight, and easy to use. See Brief for Criminal Law Professors as *Amici Curiae* 9. They may not be a complete answer to the problem, see Ayers 32, but at least for now they provide a reasonable response. In fact, a number of law enforcement agencies around the country already encourage the use of

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

Faraday bags. See, *e.g.*, Dept. of Justice, National Institute of Justice, Electronic Crime Scene Investigation: A Guide for First Responders 14, 32 (2d ed. Apr. 2008); Brief for Criminal Law Professors as *Amici Curiae* 4–6.

To the extent that law enforcement still has specific concerns about the potential loss of evidence in a particular case, there remain more targeted ways to address those concerns. If "the police are truly confronted with a 'now or never' situation,"—for example, circumstances suggesting that a defendant's phone will be the target of an imminent remote-wipe attempt—they may be able to rely on exigent circumstances to search the phone immediately. *Missouri v. McNeely*, 569 U.S. ——, ——, 133 S.Ct. 1552, 1561–1562, 185 L.Ed.2d 696 (2013) (quoting *Roaden v. Kentucky*, 413 U.S. 496, 505, 93 S.Ct. 2796, 37 L.Ed.2d 757 (1973); some internal quotation marks omitted). Or, if officers happen to seize a phone in an unlocked state, they may be able to disable a phone's automatic-lock feature in order to prevent the phone from locking and encrypting data. See App. to Reply Brief in No. 13–132, p. 3a (diagramming the few necessary steps). Such a preventive measure could ***2488** be analyzed under the principles set forth in our decision in *McArthur*, 531 U.S. 326, 121 S.Ct. 946, which approved officers' reasonable steps to secure a scene to preserve evidence while they awaited a warrant. See *id.*, at 331–333, 121 S.Ct. 946.

B

[11] The search incident to arrest exception rests not only on the heightened government interests at stake in a volatile arrest situation, but also on an arrestee's reduced privacy interests upon being taken into police custody. *Robinson* focused primarily on the first of those rationales. But it also quoted with approval then-Judge Cardozo's account of the historical basis for the search incident to arrest exception: "Search of the person becomes lawful when grounds for arrest and accusation have been discovered, and the law is in the act of subjecting the body of the accused to its physical dominion." 414 U.S., at 232, 94 S.Ct. 467 (quoting *People v. Chiagles*, 237 N.Y. 193, 197, 142 N.E. 583, 584 (1923)); see also 414 U.S., at 237, 94 S.Ct. 467 (Powell, J., concurring) ("an individual lawfully subjected to a custodial arrest retains no significant Fourth Amendment interest in the privacy of his person"). Put simply, a patdown of Robinson's clothing and an inspection of the cigarette pack found in his pocket constituted only minor additional intrusions compared to the substantial government authority exercised in taking Robinson into custody. See *Chadwick*, 433 U.S., at 16, n. 10, 97 S.Ct. 2476 (searches of a person are justified in part by "reduced expectations of privacy caused by the arrest").

[12] The fact that an arrestee has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely. Not every search "is acceptable solely because a person is in custody." *Maryland v. King*, 569 U.S. ——, ——, 133 S.Ct. 1958, 1979, 186 L.Ed.2d 1 (2013). To the contrary, when "privacy-related concerns are weighty enough" a "search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee." *Ibid.* One such example, of course, is *Chimel*. *Chimel* refused to "characteriz[e] the invasion of privacy that results from a top-to-bottom search of a man's house as 'minor.' " 395 U.S., at 766–767, n. 12, 89 S.Ct. 2034. Because a search of the arrestee's entire house was a substantial invasion beyond the arrest itself, the Court concluded that a warrant was required.

Robinson is the only decision from this Court applying *Chimel* to a search of the contents of an item found on an arrestee's person. In an earlier case, this Court had approved a search of a zipper bag carried by an arrestee, but the Court analyzed only the validity of the arrest itself. See *Draper v. United States*, 358 U.S. 307, 310–311, 79 S.Ct. 329, 3 L.Ed.2d 327 (1959). Lower courts applying *Robinson* and *Chimel*, how-

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

ever, have approved searches of a variety of personal items carried by an arrestee. See, *e.g.*, *United States v. Carrion*, 809 F.2d 1120, 1123, 1128 (C.A.5 1987) (billfold and address book); *United States v. Watson*, 669 F.2d 1374, 1383–1384 (C.A.11 1982) (wallet); *United States v. Lee*, 501 F.2d 890, 892 (C.A.D.C.1974) (purse).

[13] The United States asserts that a search of all data stored on a cell phone is "materially indistinguishable" from searches of these sorts of physical items. Brief for United States in No. 13–212, p. 26. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those ***2489** implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.

1

Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.

One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. See Kerr, Foreword: Accounting for Technological Change, 36 Harv. J.L. & Pub. Pol'y 403, 404–405 (2013). Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant in *Chadwick*, *supra*, rather than a container the size of the cigarette package in *Robinson*.

But the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones. The current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos. See Kerr, *supra*, at 404; Brief for Center for Democracy & Technology et al. as *Amici Curiae* 7–8. Cell phones couple that capacity with the ability to store many different types of information: Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on. See *id.*, at 30; *United States v. Flores–Lopez*, 670 F.3d 803, 806 (C.A.7 2012). We expect that the gulf between physical practicability and digital capacity will only continue to widen in the future.

The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.[FN1]

FN1. Because the United States and California agree that these cases involve *searches* incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances.

***2490** Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower. See Harris Interactive, 2013 Mobile Consumer Habits Study (June 2013). A decade ago police officers searching an arrestee might have occasionally stumbled across a highly personal item such as a diary. See, *e.g.*, *United States v. Frankenberry*, 387 F.2d 337 (C.A.2 1967) (*per curiam*). But those discoveries were likely to be few and far between. Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. See *Ontario v. Quon*, 560 U.S. 746, 760, 130 S.Ct. 2619, 177 L.Ed.2d 216 (2010). Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.

Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building. See *United States v. Jones*, 565 U.S. ——, ——, 132 S.Ct. 945, 955, 181 L.Ed.2d 911 (2012) (SOTOMAYOR, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.").

Mobile application software on a cell phone, or "apps," offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely. There are over a million apps available in each of the two major app stores; the phrase "there's an app for that" is now part of the popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life. See Brief for Electronic Privacy Information Center as *Amicus Curiae* in No. 13–132, p. 9.

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

In 1926, Learned Hand observed (in an opinion later quoted in *Chimel*) that it is "a totally different thing to search a man's ***2491** pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." *United States v. Kirschenblatt,* 16 F.2d 202, 203 (C.A.2). If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.

2

To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself. Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. See *New York v. Belton,* 453 U.S. 454, 460, n. 4, 101 S.Ct. 2860, 69 L.Ed.2d 768 (1981) (describing a "container" as "any object capable of holding another object"). But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen. That is what cell phones, with increasing frequency, are designed to do by taking advantage of "cloud computing." Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference. See Brief for Electronic Privacy Information Center in No. 13–132, at 12–14, 20. Moreover, the same type of data may be stored locally on the device for one user and in the cloud for another.

The United States concedes that the search incident to arrest exception may not be stretched to cover a search of files accessed remotely—that is, a search of files stored in the cloud. See Brief for United States in No. 13–212, at 43–44. Such a search would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house. But officers searching a phone's data would not typically know whether the information they are viewing was stored locally at the time of the arrest or has been pulled from the cloud.

Although the Government recognizes the problem, its proposed solutions are unclear. It suggests that officers could disconnect a phone from the network before searching the device—the very solution whose feasibility it contested with respect to the threat of remote wiping. Compare Tr. of Oral Arg. in No. 13–132, at 50–51, with Tr. of Oral Arg. in No. 13–212, pp. 13–14. Alternatively, the Government proposes that law enforcement agencies "develop protocols to address" concerns raised by cloud computing. Reply Brief in No. 13–212, pp. 14–15. Probably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols. The possibility that a search might extend well beyond papers and effects in the physical proximity of an arrestee is yet another reason that the privacy interests here dwarf those in *Robinson.*

C

Apart from their arguments for a direct extension of *Robinson,* the United States and California offer various fallback options for permitting warrantless cell phone searches under certain circumstances. Each of the proposals is flawed and contravenes our general preference to provide clear guidance to law enforcement through categorical rules. "[I]f police are to have workable rules, the balancing of the competing interests ... 'must in large part be ***2492** done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers.' " *Michigan v. Summers,* 452 U.S. 692, 705, n. 19, 101 S.Ct. 2587, 69 L.Ed.2d 340 (1981) (quoting *Dunaway v. New York,* 442 U.S.

200, 219–220, 99 S.Ct. 2248, 60 L.Ed.2d 824 (1979) (White, J., concurring)).

[14] The United States first proposes that the *Gant* standard be imported from the vehicle context, allowing a warrantless search of an arrestee's cell phone whenever it is reasonable to believe that the phone contains evidence of the crime of arrest. But *Gant* relied on "circumstances unique to the vehicle context" to endorse a search solely for the purpose of gathering evidence. 556 U.S., at 343, 129 S.Ct. 1710. Justice SCALIA's *Thornton* opinion, on which *Gant* was based, explained that those unique circumstances are "a reduced expectation of privacy" and "heightened law enforcement needs" when it comes to motor vehicles. 541 U.S., at 631, 124 S.Ct. 2127; see also *Wyoming v. Houghton*, 526 U.S., at 303–304, 119 S.Ct. 1297. For reasons that we have explained, cell phone searches bear neither of those characteristics.

At any rate, a *Gant* standard would prove no practical limit at all when it comes to cell phone searches. In the vehicle context, *Gant* generally protects against searches for evidence of past crimes. See 3 W. LaFave, Search and Seizure § 7.1(d), at 709, and n. 191. In the cell phone context, however, it is reasonable to expect that incriminating information will be found on a phone regardless of when the crime occurred. Similarly, in the vehicle context *Gant* restricts broad searches resulting from minor crimes such as traffic violations. See *id.*, § 7.1(d), at 713, and n. 204. That would not necessarily be true for cell phones. It would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone. Even an individual pulled over for something as basic as speeding might well have locational data dispositive of guilt on his phone. An individual pulled over for reckless driving might have evidence on the phone that shows whether he was texting while driving. The sources of potential pertinent information are virtually unlimited, so applying the *Gant* standard to cell phones would in effect give "police officers unbridled discretion to rummage at will among a person's private effects." 556 U.S., at 345, 129 S.Ct. 1710.

[15] The United States also proposes a rule that would restrict the scope of a cell phone search to those areas of the phone where an officer reasonably believes that information relevant to the crime, the arrestee's identity, or officer safety will be discovered. See Brief for United States in No. 13–212, at 51–53. This approach would again impose few meaningful constraints on officers. The proposed categories would sweep in a great deal of information, and officers would not always be able to discern in advance what information would be found where.

[16] We also reject the United States' final suggestion that officers should always be able to search a phone's call log, as they did in Wurie's case. The Government relies on *Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), which held that no warrant was required to use a pen register at telephone company premises to identify numbers dialed by a particular caller. The Court in that case, however, concluded that the use of a pen register was not a "search" at all under the Fourth Amendment. See *id.*, at 745–746, 99 S.Ct. 2577. There is no dispute here that the officers engaged in a search of Wurie's cell ***2493** phone. Moreover, call logs typically contain more than just phone numbers; they include any identifying information that an individual might add, such as the label "my house" in Wurie's case.

[17] Finally, at oral argument California suggested a different limiting principle, under which officers could search cell phone data if they could have obtained the same information from a pre-digital counterpart. See Tr. of Oral Arg. in No. 13–132, at 38–43; see also *Flores–Lopez*, 670 F.3d, at 807 ("If police are entitled to open a pocket diary to copy the owner's address, they should be entitled to turn on a

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

cell phone to learn its number."). But the fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery. The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years. And to make matters worse, such an analogue test would allow law enforcement to search a range of items contained on a phone, even though people would be unlikely to carry such a variety of information in physical form. In Riley's case, for example, it is implausible that he would have strolled around with video tapes, photo albums, and an address book all crammed into his pockets. But because each of those items has a pre-digital analogue, police under California's proposal would be able to search a phone for all of those items—a significant diminution of privacy.

In addition, an analogue test would launch courts on a difficult line-drawing expedition to determine which digital files are comparable to physical records. Is an e-mail equivalent to a letter? Is a voicemail equivalent to a phone message slip? It is not clear how officers could make these kinds of decisions before conducting a search, or how courts would apply the proposed rule after the fact. An analogue test would "keep defendants and judges guessing for years to come." *Sykes v. United States*, 564 U.S. 1, ——, 131 S.Ct. 2267, 2287, 180 L.Ed.2d 60 (2011)(SCALIA, J., dissenting) (discussing the Court's analogue test under the Armed Career Criminal Act).

IV

We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.

Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest. Our cases have historically recognized that the warrant requirement is "an important working part of our machinery of government," not merely "an inconvenience to be somehow 'weighed' against the claims of police efficiency." *Coolidge v. New Hampshire*, 403 U.S. 443, 481, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971). Recent technological advances similar to those discussed here have, in addition, made the process of obtaining a warrant itself more efficient. See *McNeely*, 569 U.S., at ——, 133 S.Ct., at 1561–1563; *id.*, at ——, 133 S.Ct., at 1573 (ROBERTS, C.J., concurring in part and dissenting in part) (describing jurisdiction where "police officers can e-mail warrant requests to judges' iPads [and] judges have signed such warrants and e-mailed them back to officers in less than 15 minutes").

***2494** [18] Moreover, even though the search incident to arrest exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone. "One well-recognized exception applies when ' "the exigencies of the situation" make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment.' " *Kentucky v. King*, 563 U.S., at ——, 131 S.Ct., at 1856 (quoting *Mincey v. Arizona*, 437 U.S. 385, 394, 98 S.Ct. 2408, 57 L.Ed.2d 290 (1978)). Such exigencies could include the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury. 563 U.S., at ——, 131 S.Ct. 1849. In *Chadwick*, for example, the Court held that the exception for searches incident to arrest did not justify a search of the trunk at issue, but noted that "if officers have reason to believe that luggage contains some immediately dangerous instrumentality, such as explosives, it would be foolhardy to transport it to the station house without

opening the luggage." 433 U.S., at 15, n. 9, 97 S.Ct. 2476.

[19] In light of the availability of the exigent circumstances exception, there is no reason to believe that law enforcement officers will not be able to address some of the more extreme hypotheticals that have been suggested: a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb, or a child abductor who may have information about the child's location on his cell phone. The defendants here recognize—indeed, they stress—that such fact-specific threats may justify a warrantless search of cell phone data. See Reply Brief in No. 13–132, at 8–9; Brief for Respondent in No. 13–212, at 30, 41. The critical point is that, unlike the search incident to arrest exception, the exigent circumstances exception requires a court to examine whether an emergency justified a warrantless search in each particular case. See *McNeely*, *supra*, at ——, 133 S.Ct., at 1559.[FN2]

FN2. In Wurie's case, for example, the dissenting First Circuit judge argued that exigent circumstances could have justified a search of Wurie's phone. See 728 F.3d 1, 17 (2013) (opinion of Howard, J.) (discussing the repeated unanswered calls from "my house," the suspected location of a drug stash). But the majority concluded that the Government had not made an exigent circumstances argument. See *id.*, at 1. The Government acknowledges the same in this Court. See Brief for United States in No. 13–212, p. 28, n. 8.

* * *

Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled "general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself. In 1761, the patriot James Otis delivered a speech in Boston denouncing the use of writs of assistance. A young John Adams was there, and he would later write that "[e]very man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance." 10 Works of John Adams 247–248 (C. Adams ed. 1856). According to Adams, Otis's speech was "the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born." *Id.*, at 248 (quoted in *Boyd v. United States*, 116 U.S. 616, 625, 6 S.Ct. 524, 29 L.Ed. 746 (1886)).

Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold ***2495** for many Americans "the privacies of life," *Boyd*, *supra*, at 630, 6 S.Ct. 524. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.

We reverse the judgment of the California Court of Appeal in No. 13–132 and remand the case for further proceedings not inconsistent with this opinion. We affirm the judgment of the First Circuit in No. 13–212.

It is so ordered.

Justice ALITO, concurring in part and concurring in the judgment.

I agree with the Court that law enforcement officers, in conducting a lawful search incident to arrest, must generally obtain a warrant before searching information stored or accessible on a cell phone. I write

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

separately to address two points.

I

A

First, I am not convinced at this time that the ancient rule on searches incident to arrest is based exclusively (or even primarily) on the need to protect the safety of arresting officers and the need to prevent the destruction of evidence. Cf. *ante,* at 2484. This rule antedates the adoption of the Fourth Amendment by at least a century. See T. Clancy, The Fourth Amendment: Its History and Interpretation 340 (2008); T. Taylor, Two Studies in Constitutional Interpretation 28 (1969); Amar, Fourth Amendment First Principles, 107 Harv. L. Rev. 757, 764 (1994). In *Weeks v. United States*, 232 U.S. 383, 392, 34 S.Ct. 341, 58 L.Ed. 652 (1914), we held that the Fourth Amendment did not disturb this rule. See also Taylor, *supra,* at 45; Stuntz, The Substantive Origins of Criminal Procedure, 105 Yale L.J. 393, 401 (1995) ("The power to search incident to arrest—a search of the arrested suspect's person ...—was well established in the mid-eighteenth century, and nothing in ... the Fourth Amendment changed that"). And neither in *Weeks* nor in any of the authorities discussing the old common-law rule have I found any suggestion that it was based exclusively or primarily on the need to protect arresting officers or to prevent the destruction of evidence.

On the contrary, when pre- *Weeks* authorities discussed the basis for the rule, what was mentioned was the need to obtain probative evidence. For example, an 1839 case stated that "it is clear, and beyond doubt, that ... constables ... are entitled, upon a lawful arrest by them of one charged with treason or felony, to take and detain property found in his possession which will form material evidence in his prosecution for that crime." See *Dillon v. O'Brien,* 16 Cox Crim. Cas. 245, 249–251 (1887) (citing *Regina,* v. *Frost,* 9 Car. & P. 129, 173 Eng. Rep. 771). The court noted that the origins of that rule "deriv[e] from the interest which the State has in a person guilty (or reasonably believed to be guilty) of a crime being brought to justice, and in a prosecution, once commenced, being determined in due course of law." 16 Cox Crim. Cas., at 249–250. See also *Holker v. Hennessey,* 141 Mo. 527, 537–540, 42 S.W. 1090, 1093 (1897).

Two 19th-century treatises that this Court has previously cited in connection with the origin of the search-incident-to-arrest rule, see *Weeks, supra,* at 392, 34 S.Ct. 341, suggest the same rationale. See F. Wharton, Criminal Pleading and Practice § 60, p. 45 (8th ed. 1880) ("Those ***2496** arresting a defendant are bound to take from his person any articles which may be of use as proof in the trial of the offense with which the defendant is charged"); J. Bishop, Criminal Procedure §§ 210–212, p. 127 (2d ed. 1872) (if an arresting officer finds "about the prisoner's person, or otherwise in his possession, either goods or moneys which there is reason to believe are connected with the supposed crime as its fruits, or as the instruments with which it was committed, or as directly furnishing evidence relating to the transaction, he may take the same, and hold them to be disposed of as the court may direct").

What ultimately convinces me that the rule is not closely linked to the need for officer safety and evidence preservation is that these rationales fail to explain the rule's well-recognized scope. It has long been accepted that written items found on the person of an arrestee may be examined and used at trial.[FN*] But once these items are taken away from an arrestee (something that obviously must be done before the items are read), there is no risk that the arrestee will destroy them. Nor is there any risk that leaving these items unread will endanger the arresting officers.

FN* Cf. *Hill v. California,* 401 U.S. 797, 799–802, and n. 1, 91 S.Ct. 1106, 28 L.Ed.2d 484 (1971) (diary); *Marron v. United States,* 275 U.S. 192, 193, 198–199, 48 S.Ct. 74, 72 L.Ed. 231 (1927) (ledger and bills); *Gouled*

v. United States, 255 U.S. 298, 309, 41 S.Ct. 261, 65 L.Ed. 647 (1921), overruled on other grounds, *Warden, Md. Penitentiary v. Hayden,* 387 U.S. 294, 300–301, 87 S.Ct. 1642, 18 L.Ed.2d 782 (1967) (papers); see *United States v. Rodriguez,* 995 F.2d 776, 778 (C.A.7 1993) (address book); *United States v. Armendariz–Mata,* 949 F.2d 151, 153 (C.A.5 1991) (notebook); *United States v. Molinaro,* 877 F.2d 1341 (C.A.7 1989) (wallet); *United States v. Richardson,* 764 F.2d 1514, 1527 (C.A.11 1985) (wallet and papers); *United States v. Watson,* 669 F.2d 1374, 1383–1384 (C.A.11 1982) (documents found in a wallet); *United States v. Castro,* 596 F.2d 674, 677 (C.A.5 1979), cert. denied, 444 U.S. 963, 100 S.Ct. 448, 62 L.Ed.2d 375 (1979) (paper found in a pocket); *United States v. Jeffers,* 520 F.2d 1256, 1267–1268 (C.A.7 1975) (three notebooks and meeting minutes); *Bozel v. Hudspeth,* 126 F.2d 585, 587 (C.A.10 1942) (papers, circulars, advertising matter, "memoranda containing various names and addresses"); *United States v. Park Avenue Pharmacy,* 56 F.2d 753, 755 (C.A.2 1932) ("numerous prescriptions blanks" and a check book). See also 3 W. LaFave, Search and Seizure § 5.2(c), p. 144 (5th ed. 2012) ("Lower courts, in applying Robinson, have deemed evidentiary searches of an arrested person to be virtually unlimited"); W. Cuddihy, Fourth Amendment: Origins and Original Meaning 847–848 (1990) (in the pre-Constitution colonial era, "[a]nyone arrested could expect that not only his surface clothing but his body, luggage, and saddlebags would be searched").

The idea that officer safety and the preservation of evidence are the sole reasons for allowing a warrantless search incident to arrest appears to derive from the Court's reasoning in *Chimel v. California,* 395 U.S. 752, 89 S.Ct. 2034, 23 L.Ed.2d 685 (1969), a case that involved the lawfulness of a search of the scene of an arrest, not the person of an arrestee. As I have explained, *Chimel* 's reasoning is questionable, see *Arizona v. Gant,* 556 U.S. 332, 361–363, 129 S.Ct. 1710, 173 L.Ed.2d 485 (2009) (ALITO, J., dissenting), and I think it is a mistake to allow that reasoning to affect cases like these that concern the search of the person of arrestees.

B

Despite my view on the point discussed above, I agree that we should not mechanically apply the rule used in the predigital era to the search of a cell phone. Many cell phones now in use are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form. This calls for a new balancing***2497** of law enforcement and privacy interests.

The Court strikes this balance in favor of privacy interests with respect to all cell phones and all information found in them, and this approach leads to anomalies. For example, the Court's broad holding favors information in digital form over information in hard-copy form. Suppose that two suspects are arrested. Suspect number one has in his pocket a monthly bill for his land-line phone, and the bill lists an incriminating call to a long-distance number. He also has in his a wallet a few snapshots, and one of these is incriminating. Suspect number two has in his pocket a cell phone, the call log of which shows a call to the same incriminating number. In addition, a number of photos are stored in the memory of the cell phone, and one of these is incriminating. Under established law, the police may seize and examine the phone bill and the snapshots in the wallet without obtaining a warrant, but under the Court's holding today, the information stored in the cell phone is out.

While the Court's approach leads to anomalies, I do not see a workable alternative. Law enforcement

134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Dail Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921
(Cite as: 134 S.Ct. 2473)

officers need clear rules regarding searches incident to arrest, and it would take many cases and many years for the courts to develop more nuanced rules. And during that time, the nature of the electronic devices that ordinary Americans carry on their persons would continue to change.

II

This brings me to my second point. While I agree with the holding of the Court, I would reconsider the question presented here if either Congress or state legislatures, after assessing the legitimate needs of law enforcement and the privacy interests of cell phone owners, enact legislation that draws reasonable distinctions based on categories of information or perhaps other variables.

The regulation of electronic surveillance provides an instructive example. After this Court held that electronic surveillance constitutes a search even when no property interest is invaded, see *Katz v. United States*, 389 U.S. 347, 353–359, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), Congress responded by enacting Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 82 Stat. 211. See also 18 U.S.C. § 2510 *et seq.* Since that time, electronic surveillance has been governed primarily, not by decisions of this Court, but by the statute, which authorizes but imposes detailed restrictions on electronic surveillance. See *ibid.*

Modern cell phones are of great value for both lawful and unlawful purposes. They can be used in committing many serious crimes, and they present new and difficult law enforcement problems. See Brief for United States in No. 13–212, pp. 2–3. At the same time, because of the role that these devices have come to play in contemporary life, searching their contents implicates very sensitive privacy interests that this Court is poorly positioned to understand and evaluate. Many forms of modern technology are making it easier and easier for both government and private entities to amass a wealth of information about the lives of ordinary Americans, and at the same time, many ordinary Americans are choosing to make public much information that was seldom revealed to outsiders just a few decades ago.

In light of these developments, it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred ***2498** and those that almost certainly will take place in the future.

U.S.Cal.,2014.
Riley v. California
134 S.Ct. 2473, 189 L.Ed.2d 430, 82 USLW 4558, 42 Media L. Rep. 1925, 14 Cal. Daily Op. Serv. 7045, 2014 Daily Journal D.A.R. 8220, 60 Communications Reg. (P&F) 1175, 24 Fla. L. Weekly Fed. S 921

END OF DOCUMENT

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

Court of Appeal, Third District, California.
Gina M. HOLMES, Plaintiff and Appellant,
v.
PETROVICH DEVELOPMENT COMPANY, LLC, et al., Defendants and Respondents.

No. C059133.
Jan. 13, 2011.

Background: Employee brought action against employer and supervisor for sexual harassment, retaliation, wrongful termination, violation of the right to privacy, and intentional infliction of emotional distress. The Superior Court, Sacramento County, No. 05AS04356,Chang and Jones, JJ., granted summary adjudication with respect to the causes of action for discrimination, retaliation, and wrongful termination, and entered judgment on jury verdict for defendants as to the two remaining causes of action. Employee appealed.

Holdings: The Court of Appeal, Scotland, J., held that:
(1) no reasonable jury could find that employee's work environment was objectively hostile;
(2) supervisor's acts were not an “adverse employment action” as required for retaliation;
(3) attorney-client communications over work computer were not privileged; and
(4) admonishment to jury that attorney-client communications over work computer were not privileged did not improperly undermine employee's invasion of privacy claim.

Affirmed.

West Headnotes

[1] Appeal and Error 30 901

30 Appeal and Error
30XVI Review
30XVI(G) Presumptions
30k901 k. Burden of showing error. Most Cited Cases

Appeal and Error 30 934(1)

30 Appeal and Error
30XVI Review
30XVI(G) Presumptions
30k934 Judgment
30k934(1) k. In general. Most Cited Cases

Reviewing courts must presume the judgment is correct, and the appellant bears the burden of demonstrating error.

[2] Civil Rights 78 1184

78 Civil Rights
78II Employment Practices
78k1181 Sexual Harassment; Work Environment
78k1184 k. Quid pro quo. Most Cited Cases

Civil Rights 78 1185

78 Civil Rights
78II Employment Practices
78k1181 Sexual Harassment; Work Environment
78k1185 k. Hostile environment; severity,

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

pervasiveness, and frequency. Most Cited Cases

There are two theories upon which sexual harassment may be alleged under Fair Employment and Housing Act (FEHA): quid pro quo harassment, where a term of employment is conditioned upon submission to unwelcome sexual advances; and hostile work environment, where the harassment is sufficiently pervasive so as to alter the conditions of employment and create an abusive work environment. West's Ann.Cal.Gov.Code § 12940(j).

[3] Civil Rights 78 1185

78 Civil Rights
78II Employment Practices
78k1181 Sexual Harassment; Work Environment
78k1185 k. Hostile environment; severity, pervasiveness, and frequency. Most Cited Cases

To prevail on a claim of hostile work environment sexual harassment, an employee must demonstrate that he or she was subjected to sexual advances, conduct, or comments that were (1) unwelcome, (2) because of sex, and (3) sufficiently severe or pervasive to alter the conditions of his or her employment and create an abusive work environment. West's Ann.Cal.Gov.Code § 12940(j).

[4] Civil Rights 78 1147

78 Civil Rights
78II Employment Practices
78k1143 Harassment; Work Environment
78k1147 k. Hostile environment; severity, pervasiveness, and frequency. Most Cited Cases

Whether an environment is "hostile" or "abusive" in violation of Fair Employment and Housing Act (FEHA) can be determined only by looking at all the circumstances including the frequency of the discriminatory conduct; its severity; whether it is physically threatening or humiliating, or a mere offensive utterance; and whether it unreasonably interferes with an employee's work performance. West's Ann.Cal.Gov.Code § 12940.

[5] Civil Rights 78 1185

78 Civil Rights
78II Employment Practices
78k1181 Sexual Harassment; Work Environment
78k1185 k. Hostile environment; severity, pervasiveness, and frequency. Most Cited Cases

To establish liability in a Fair Employment and Housing Act (FEHA) hostile work environment sexual harassment case, a plaintiff employee must show she was subjected to sexual advances, conduct, or comments that were severe enough or sufficiently pervasive to alter the conditions of her employment and create a hostile or abusive work environment. West's Ann.Cal.Gov.Code § 12940(j)(4)(C).

[6] Civil Rights 78 1185

78 Civil Rights
78II Employment Practices
78k1181 Sexual Harassment; Work Environment
78k1185 k. Hostile environment; severity, pervasiveness, and frequency. Most Cited Cases

To be actionable under Fair Employment and Housing Act (FEHA), a sexually objectionable environment must be both objectively and subjectively offensive, one that a reasonable person would find hostile or abusive, and one that the victim in fact did perceive to be so. West's Ann.Cal.Gov.Code § 12940(j)(4)(C).

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

[7] Civil Rights 78 1123

78 Civil Rights
78II Employment Practices
78k1123 k. Constructive discharge. Most Cited Cases

Civil Rights 78 1185

78 Civil Rights
78II Employment Practices
78k1181 Sexual Harassment; Work Environment
78k1185 k. Hostile environment; severity, pervasiveness, and frequency. Most Cited Cases

No reasonable jury could find that employee's work environment was objectively hostile for a reasonable pregnant woman, and thus supervisor and employer were not liable for sexual harassment or constructive discharge under Fair Employment and Housing Act (FEHA), even though supervisor stated he was offended that employee had changed the period of time she would be absent for maternity leave, stated that he felt "deceived" and "taken advantage of" because employee did not notify him of her pregnancy in her job interview, and forwarded to others employee's e-mail containing information about her prior miscarriages and the possibility she would have terminated her pregnancy, where coworkers complied when employee asked them to stop asking about employee's maternity leave, and supervisor stated he would honor employee's legal rights and he was not asking for her resignation. West's Ann.Cal.Gov.Code § 12940(j)(4)(C).

[8] Civil Rights 78 1147

78 Civil Rights
78II Employment Practices
78k1143 Harassment; Work Environment
78k1147 k. Hostile environment; severity, pervasiveness, and frequency. Most Cited Cases

There is no recovery under Fair Employment and Housing Act (FEHA) for harassment that is occasional, isolated, sporadic, or trivial; rather, a plaintiff must show a concerted pattern of harassment that is repeated, routine, or generalized in nature. West's Ann.Cal.Gov.Code § 12940(j).

[9] Labor and Employment 231H 826

231H Labor and Employment
231HVIII Adverse Employment Action
231HVIII(A) In General
231Hk823 What Constitutes Adverse Action
231Hk826 k. Constructive discharge. Most Cited Cases

"Constructive discharge" occurs only when the employer coerces the employee's resignation, either by creating working conditions that are intolerable under an objective standard, or by failing to remedy objectively intolerable working conditions that actually are known to the employer.

[10] Labor and Employment 231H 826

231H Labor and Employment
231HVIII Adverse Employment Action
231HVIII(A) In General
231Hk823 What Constitutes Adverse Action
231Hk826 k. Constructive discharge. Most Cited Cases

For constructive discharge, the conditions prompting the employee's resignation must be sufficiently extraordinary and egregious to overcome the

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

normal motivation of a competent, diligent, and reasonable employee to remain on the job.

[11] Civil Rights 78 1246

78 Civil Rights
78II Employment Practices
78k1241 Retaliation for Exercise of Rights
78k1246 k. Particular cases. Most Cited Cases

Supervisor's acts of expressing concern about employee's plan to take maternity leave sooner and for a longer period than anticipated, and forwarding to others an e-mail which contained information about employee's prior miscarriages and the possibility she would have terminated her pregnancy if amniocentesis results had revealed problems, was not an "adverse employment action," and thus could not support a claim of retaliation under Fair Employment and Housing Act (FEHA), where there was no clear directive in the e-mail that employee did not wish others to see it, and supervisor forwarded the e-mail only to people he believed needed to know that employee had changed the anticipated date of her pregnancy leave and that she might be quitting. West's Ann.Cal.Gov.Code § 12940.

[12] Labor and Employment 231H 824

231H Labor and Employment
231HVIII Adverse Employment Action
231HVIII(A) In General
231Hk823 What Constitutes Adverse Action
231Hk824 k. In general. Most Cited Cases

An "adverse employment action," which is a critical component of a retaliation claim, requires a substantial adverse change in the terms and conditions of the plaintiff's employment.

[13] Civil Rights 78 1245

78 Civil Rights
78II Employment Practices
78k1241 Retaliation for Exercise of Rights
78k1245 k. Adverse actions in general. Most Cited Cases

A mere offensive utterance or a pattern of social slights by either the employer or coemployees cannot properly be viewed as materially affecting the terms, conditions, or privileges of employment for purposes of the Fair Employment and Housing Act (FEHA), and thus is not an adverse employment action as required for a retaliation claim. West's Ann.Cal.Gov.Code § 12940.

[14] Civil Rights 78 1245

78 Civil Rights
78II Employment Practices
78k1241 Retaliation for Exercise of Rights
78k1245 k. Adverse actions in general. Most Cited Cases

A series of alleged discriminatory acts must be considered collectively rather than individually in determining whether the overall employment action is adverse and, in the end, the determination of whether there was an adverse employment action as required for a retaliation claim is made on a case-by-case basis, in light of the objective evidence. West's Ann.Cal.Gov.Code § 12940.

[15] Appeal and Error 30 762

30 Appeal and Error
30XII Briefs
30k762 k. Reply briefs. Most Cited Cases

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

Employee's failure to raise the argument earlier than in her reply brief, or to make a showing of good cause, forfeited the argument on appeal that trial court should have denied employer's motion for summary adjudication of employee's Fair Employment and Housing Act (FEHA) claims in its entirety because it was not timely served. West's Ann.Cal.Gov.Code § 12940.

[16] Appeal and Error 30 762

30 Appeal and Error
30XII Briefs
30k762 k. Reply briefs. Most Cited Cases

Points raised for the first time in a reply brief will ordinarily not be considered, because such consideration would deprive the respondent of an opportunity to counter the argument.

[17] Appearance 31 24(10)

31 Appearance
31k21 Waiver of Objections
31k24 Defects in Process or Service
31k24(10) k. Motions. Most Cited Cases

Trial court did not err in ruling that employee's acts of filing an opposition and appearing at the hearing on employer's motion for summary adjudication of employee's Fair Employment and Housing Act (FEHA) claims waived the defect in employer's alleged failure to timely serve the motion. West's Ann.Cal.Gov.Code § 12940.

[18] Privileged Communications and Confidentiality 311H 168

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk168 k. Waiver of privilege. Most Cited Cases

Privileged Communications and Confidentiality 311H 176

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk175 Determination
311Hk176 k. In general. Most Cited Cases

Trial court made a finding that employee waived the attorney-client privilege as to e-mails sent from employer's computer, even though employer's objections to the claim of attorney-client privilege were made on multiple grounds, and the court merely sustained the objection without specifying the basis for its ruling, where the trial court stated in connection with a motion for discovery sanctions that the court had found employee had waived the attorney-client privilege, and the same judge ruled on both the objection and the motion for discovery sanctions. West's Ann.Cal.Evid.Code § 954.

[19] Privileged Communications and Confidentiality 311H 141

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk135 Mode or Form of Communications
311Hk141 k. E-mail and electronic communication. Most Cited Cases

Privileged Communications and Confidentiality 311H 156

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk156 k. Confidential character of communications or advice. Most Cited Cases

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

In the context of a client's future lawsuit against the owner of an electronic means of communication, an electronic communication between the client and an attorney is not a "confidential communication between client and lawyer" within meaning of privilege statute, when (1) the owner's electronic means is used to make the communication; (2) the owner has advised the client that communications using electronic means are not private, may be monitored, and may be used only for business purposes; and (3) the client is aware of and agrees to these conditions. West's Ann.Cal.Evid.Code §§ 917(b), 952.

[20] Privileged Communications and Confidentiality 311H 141

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk135 Mode or Form of Communications
311Hk141 k. E-mail and electronic communication. Most Cited Cases

Privileged Communications and Confidentiality 311H 156

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk156 k. Confidential character of communications or advice. Most Cited Cases

Client did not have a reasonable expectation of privacy in her communications with her attorney using her employer's company e-mail account and her employer's computer, and thus the communications were not covered by attorney-client privilege in employee's subsequent lawsuit against employer and supervisor, even though employee utilized a private password to use the computer and she deleted the e-mails after they were sent, where employee had been warned that the account was to be used only for company business, that e-mails were not private, and that the company would randomly and periodically monitor its technology resources to ensure compliance with the policy, absent evidence that employee knew for a fact that employer never actually monitored e-mail. West's Ann.Cal.Evid.Code §§ 917(b), 952.

See Cal. Jur. 3d, Evidence, § 522; Cal. Civil Practice (Thomson Reuters 2010) Procedure, § 13:6; Weil & Brown, Cal. Practice Guide: Civil Procedure Before Trial (The Rutter Group 2010) ¶ 8:199.20 (CACIVP Ch. 8C-3); Wegner et al., Cal. Practice Guide: Civil Trials and Evidence (The Rutter Group 2010) ¶ 8:1927.5, 8:2028.2 (CACIVEV Ch. 8E-A); 2 Witkin, Cal. Evidence (4th ed. 2000) Witnesses, §§ 75, 76.

[21] Privileged Communications and Confidentiality 311H 141

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk135 Mode or Form of Communications
311Hk141 k. E-mail and electronic communication. Most Cited Cases

Privileged Communications and Confidentiality 311H 156

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk156 k. Confidential character of communications or advice. Most Cited Cases

In determining whether an employee had a reasonable expectation of privacy in communications using company computers sufficient to support the attorney-client privilege, absent a company communication to employees explicitly contradicting the company's warning to them that company computers are monitored to make sure employees are not using them to send personal e-mail, it is immaterial that the "operational reality" is the company does not actually do so. West's Ann.Cal.Evid.Code §§ 917(b), 952.

[22] Trial 388 29(2)

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

388 Trial
388III Course and Conduct of Trial in General
388k29 Remarks of Judge
388k29(2) k. Comments on evidence. Most Cited Cases

Trial court's protective admonishment to jury, stating that attorney-client e-mails sent by employee were not privileged because they were sent from a company computer, did not improperly undermine employee's invasion of privacy claim against employer by advising the jury employee had no right to privacy in e-mails on a company computer, where employee's claim was based on supervisor's act of forwarding an e-mail that was not an attorney-client communication, and trial court stated that its determination about privilege had "nothing whatsoever to do with" employee's privacy claim. West's Ann.Cal. Const. Art. 1, § 1; West's Ann.Cal.Evid.Code §§ 917(b), 952.

[23] Appeal and Error 30 1046.5

30 Appeal and Error
30XVI Review
30XVI(J) Harmless Error
30XVI(J)7 Conduct of Trial or Hearing
30k1046.5 k. Remarks and conduct of judge. Most Cited Cases

Employee failed to meet her burden of establishing that the alleged error was prejudicial to her invasion of privacy claim, in trial court's admonishment to jury that attorney-client e-mails sent by employee were not privileged because they were sent from a company computer, where employee did not present a coherent argument explaining how the court's statement undermined her theory that supervisor egregiously violated her privacy by forwarding e-mails about her difficult and sensitive pregnancy decisions to people she claimed had no legitimate business need to know about the matters discussed therein. West's Ann.Cal. Const. Art. 1, § 1; West's Ann.Cal.Evid.Code §§ 917(b), 952.

[24] Appeal and Error 30 762

30 Appeal and Error
30XII Briefs
30k762 k. Reply briefs. Most Cited Cases

Employee's failure to raise the arguments earlier than in her reply brief, in challenging jury's verdict for employer on employee's cause of action for invasion of privacy, forfeited the arguments on appeal that "an employer cannot destroy the constitutional right to privacy via a company handbook without due consideration being paid," that "an employee has a reasonable expectation of privacy when an employer's technology policy is not enforced," and that "an employer violates an employee's right to privacy when he discloses private information about the employee without a legitimate business reason for doing so." West's Ann.Cal. Const. Art. 1, § 1.

****882** Joanna R. Mendoza, Law Offices of Joanna R. Mendoza, Sacramento, for Plaintiff and Appellant.

Robin K. Perkins, Perkins & Associates, Sacramento, for Defendants and Respondents.

SCOTLAND, J.[FN*]

FN* Retired Presiding Justice of the Court of Appeal, Third Appellate District, assigned by the Chief Justice pursuant to article VI, section 6 of the California Constitution.

***1051** Plaintiff Gina Holmes appeals from the judgment entered in favor of defendants Petrovich Development Company, LLC and Paul Petrovich in her lawsuit for sexual harassment, retaliation,

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

wrongful termination, violation of the right to privacy, and intentional infliction of emotional distress.[FN1] She contends that the trial court erred in granting defendants' motion for summary adjudication with respect to the causes of action for discrimination, retaliation, and wrongful termination, and that the jury's verdict as to the remaining causes of action must be reversed due to evidentiary and instructional errors. We disagree and shall affirm the judgment.

> FN1. Hereafter, we will refer to Petrovich Development Company, LLC as the company, to Paul Petrovich as Petrovich, and to them collectively as defendants.

Among other things, we conclude that e-mails sent by Holmes to her attorney regarding possible legal action against defendants did not constitute " 'confidential communication between client and lawyer' " within the meaning of ****883**Evidence Code section 952. This is so because Holmes used a computer of defendant company to send the e-mails even though (1) she had been told of the company's policy that its computers were to be used only for company business and that employees were prohibited from using them to send or receive personal e-mail, (2) she had been warned that the company would monitor its computers for compliance with this company policy and thus might "inspect all files and messages ... at any time," and (3) she had been explicitly advised that employees using company computers to create or maintain personal information or messages "have no right of privacy with respect to that information or message."

As we will explain, an attorney-client communication "does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication." (Evid.Code, § 917, subd. (b).) However, the e-mails sent via company computer under the circumstances of this case were akin to consulting her lawyer in her employer's conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard by him. By using the company's computer to communicate with her lawyer, knowing the communications violated company computer policy and could be discovered by her employer due to company monitoring of e-mail usage, Holmes did not communicate "in confidence by means which, so far as the client is aware, ***1052** discloses the information to no third persons other than those who are present to further the interest of the client in the consultation or those to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted." (Evid.Code, § 952.) Consequently, the communications were not privileged.

FACTS

Holmes began working for Petrovich as his executive assistant in early June 2004.

The employee handbook, which Holmes admitted reading and signing, contained provisions clearly spelling out the policy concerning use of the company's technology resources, such as computers and e-mail accounts. The handbook directs employees that the company's technology resources should be used only for company business and that employees are prohibited from sending or receiving personal e-mails. Moreover, the handbook warns that "[e]mployees who use the Company's Technology Resources to create or maintain personal information or messages have no right of privacy with respect to that information or message." The "Internet and Intranet Usage" policy in the handbook specifically states, "E-mail is not private communication, because others may be able to read or access the message. E-mail may best be regarded as a postcard rather than as a sealed letter...." The hand-

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

book spells out further that the company may "inspect all files or messages ... at any time for any reason at its discretion" and that it would periodically monitor its technology resources for compliance with the company's policy.

The handbook also set forth the company's policy regarding harassment and discrimination. It directs an employee who thinks that he or she has been subjected to harassment or discrimination to immediately report it to Petrovich or Cheryl Petrovich, who was the company's secretary and handled some human resources functions. If the complaining party is not comfortable****884** reporting the conduct to them, the report should be made to the company's Controller. The policy promises that the complaint will be taken seriously, it will be investigated thoroughly, and there will be no retaliation. The policy also urges the employee, when possible, to confront the person who is engaging in the unwanted conduct and ask the person to stop it.

The next month, July of 2004, Holmes told Petrovich that she was pregnant and that her due date was December 7, 2004. Petrovich recalled that Holmes told him she planned to work up until her due date and then would be out on maternity leave for six weeks.

***1053** Holmes did not like it when coworkers asked her questions about maternity leave; she thought such comments were inappropriate. She asked "[t]hat little group of hens" to stop, and they complied. Holmes recalled having about six conversations with Petrovich about her pregnancy, during which they discussed her belly getting big and baby names. She thought "belly-monitoring" comments were inappropriate, but never told Petrovich that he was being offensive.

On Friday morning, August 6, 2004, Petrovich sent Holmes an e-mail discussing various topics, including that they needed to determine how they were going to handle getting a qualified person to help in the office who would be up to speed while Holmes was on maternity leave. He explained that, given his schedule and pace, this would not be a simple task. Thus, they needed to coordinate the transition so neither he nor Holmes would be stressed about it before or after Holmes left on maternity leave. Petrovich stated: "My recollection from the email you sent me when you told me you were pregnant and in our subsequent conversations, you are due around December 7th and will be out six weeks. We are usually swamped between now and the third week of December. The good news is between the third week of December to the second week of January, it slows down a little."

Holmes e-mailed Petrovich a few hours later and advised him that she estimated starting her maternity leave around November 15, and that the time estimate of six weeks might not be accurate as she could be out for the maximum time allowed by the employee handbook and California law, which is four months. She did not expect to be gone for the full four months but thought she should mention it as a possibility. Holmes believed that "Leslie" was "capable of picking up most of the slack" while Holmes was gone, and that the company could hire a "temp just to cover some of the receptionist duties so that Leslie could be more available...."

A short time later, Petrovich responded, "I need some honesty. How pregnant were you when you interviewed with me and what happened to six weeks? Leslie is not and cannot cover your position, nor can a temp. That is an extreme hardship on me, my business and everybody else in the company. You have rights for sure and I am not going to do anything to violate any laws, but I feel taken advantage of and deceived for sure."

Holmes replied that she thought the subject was

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

better handled in person, "but here it goes anyway. [¶] I find it offensive that you feel I was dishonest or deceitful. I wrote a very detailed email explaining my pregnancy as soon as the tests from my amniocentesis came back that everything was 'normal' with the baby. An amnio cannot be performed until you are nearly 4 months pregnant, hence the delay in knowing the results. I am 39 years old, and ***1054** therefore, there was a chance that there could be something 'wrong' or 'abnormal' with the baby. If there had been, I had decided not to carry the baby to ****885** term. That is a very personal choice, and not something that I wanted to have to share with people at work; so in order to avoid that, I waited until I knew that everything was o.k. before telling anyone I was pregnant. [¶] I've also had 2 miscarriages at 3 months into my pregnancy, and could not bear having to share that with co-workers again, as I have in the past. [¶] These are very important and personal decisions that I made. I feel that I have the right to make these decisions, and there is no deceipt [*sic*] or dishonesty involved with this. On a more professional level; there is no requirement in a job interview or application to divulge if you are pregnant or not; in fact, I believe it's considered unethical to even inquire as to such. [¶] At this point, I feel that your words have put us in a bad position where our working relationship is concerned, and I don't know if we can get past it. [¶] As long as we're being straightforward with each other, please just tell me if what you are wanting at this time, is for me to not be here anymore, because that is how it feels. [¶] I need to go home and gather my thoughts."

Because he was concerned that Holmes might be quitting, Petrovich forwarded their e-mail exchange to Cheryl Petrovich; Lisa Montagnino, who handled some human resources functions; in-house counsel Bruce Stewart; and Jennifer Myers, who handled payroll and maintained employee files.

Petrovich also e-mailed Holmes as follows: "All I ever want is for people to be honest with me. The decision is all yours as to whether you stay here. I am NOT asking for your resignation. I do have the right to express my feelings, so I can't help it if you feel offended if the dates and amount of time you told me you would be out on maternity leave no longer apply. I also never asked you about you [being] pregnant in our interview, so you mentioning unethical behavior is out of place. I think you are missing the whole point here. I am trying to keep my business organized and I was working off information you told me. When you disclosed, only upon me asking, that what you told me is incorrect and that you had already decided on a maternity leave date without ever informing me, I [have] the right to question [the] information and not be subject to being quoted California law or my own handbook. You obviously are well versed on all of this which speaks volumes. No, you are not fired. Yes, you are required to be straight with your employer. If you do not wish to remain employed here, I need to know immediately."

On Monday morning, August 9, 2004, Holmes sent an e-mail to Petrovich, who was vacationing in Montana. She explained that she had thought about things a lot over the weekend and felt that what occurred on Friday could have been avoided if they had communicated in person. She enjoyed her ***1055** employment and took it as a compliment that Petrovich was worried about filling her shoes in her absence. Holmes stated, "I may only be gone 6 weeks, but I don't want to commit to that, because unforeseen circumstances can happen making my absence continue slightly longer. The max is 4 months, and that is only if there are disability issues; which I don't anticipate in my case, but I wanted to give you the 'outside' number, so you wouldn't be left with any surprises. [¶] I am happy about my pregnancy and happy about my job; I'd like to feel good about continuing to work here, in a positive and supportive environment up until my maternity leave in November, and I would like to return shortly thereafter. [¶] If we are on the same page, please let me know. I will do whatever I can to accommodate you while I'm gone; I can work from

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

home, or come in a few hours a ****886** day; I am very flexible and hope that we will be able to work out the bumps along the way."

Petrovich replied that he agreed with Holmes's e-mail and saw things the way that she did. He stated, "I agree we do need to communicate. I need [to] admit I was in shock when you told me you were pregnant so soon after you started work. Right or wrong, I felt entrapped. It's a 'no win' for an employer. Yes, I am happy for you, but it was building in me and I decide[d] to approach it by asking if your plans were still as represented. When everything got moved up, I felt even worse. I know I have no right to feel this way by law or as an employer, but I am human in a tough business where people are constantly trying to take advantage of me. Remember what I said about loyalty in our interview? The person closest to me in the office has been the person in your position. When this happened, it greatly upset me since I was hoping for the very best foundation for us since I have been pleased with your efforts and because it had been a while since I have found someone committed to do what is a tough job. It will take some time for me to 'get over it' but I will and I want you to stay. It will work."

Early the next morning, August 10, 2004, Holmes replied, "Thank you Paul. I understand your feelings, you understand mine; let's move forward in a positive direction, and remember, 'this too shall pass'." She then discussed some business matters, said that everyone was thinking of Petrovich and his family, and stated that "Norman and Oliver say meow and woof!"

At some point after she e-mailed Petrovich, Holmes learned that Petrovich had forwarded their e-mails regarding her pregnancy to Cheryl Petrovich, Bruce Stewart, Lisa Montagnino, and Jennifer Myers. Although she never asked Petrovich not to forward the e-mails to others, and she conceded the e-mails did not contain any language communicating that the information was to be kept private, Holmes was very upset because she "thought that it went without saying" the e-mails should not be disseminated to others.

***1056** On August 10, 2004, Holmes saw her doctor for routine obstetric care and complained about being harassed at work regarding her upcoming pregnancy disability leave. According to the doctor, Holmes was "moderately upset" and "somewhat tearful." He advised her that the best course of action would be to discuss the matter directly with her boss about how she feels and remedy the situation. If the harassment continued, then she might benefit from the assistance of a lawyer.

At 3:30 p.m. on the same day that Holmes saw her doctor and had e-mailed Petrovich that they could move forward in a positive direction, Holmes used the company computer to e-mail an attorney, Joanna Mendoza. Holmes asked for a referral to an attorney specializing in labor law, specifically relating to pregnancy discrimination. When Mendoza asked what was going on, Holmes replied that her boss was making it unbearable for her. He said things that were upsetting and hurtful, and had forwarded personal e-mail about her pregnancy to others in the office. Holmes stated, "I know that there are laws that protect pregnant women from being treated differently due to their pregnancy, and now that I am officially working in a hostile environment, I feel I need to find out what rights, if any, and what options I have. I don't want to quit my job; but how do I make the situation better." Holmes explained that her boss had accused her of being dishonest because she underestimated her maternity leave, that he had forwarded a personal e-mail and ****887** made it "common reading material for employees," and that he had made her feel like an "outcast." Holmes forwarded to Mendoza a few of Petrovich's e-mails.

At 4:42 p.m. on the same day, Mendoza e-mailed Holmes that she should delete their attorney-client

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

communications from her work computer because her employer might claim a right to access it. Mendoza suggested they needed to talk and, while they could talk on the phone, she "would love an excuse to see [Holmes] and catch up on everything." Mendoza stated they could meet for lunch the next day. Holmes agreed and said she would come to Mendoza's law office, at which time Mendoza could see her "big belly."

On the evening of August 11, 2004, after her lunch with Mendoza, Holmes e-mailed Petrovich saying that Holmes had been upset since his first e-mail on Friday. She had been in tears, her stomach was in knots, and she realized that they would be unable "to put this issue behind us." She stated, "I think you will understand that your feelings about my pregnancy; which you have made more than clear, leave me no alternative but to end my employment here." Holmes advised Petrovich that she had cleared her things from her desk and would not be returning to work. Holmes also e-mailed Jennifer Myers stating that she was quitting and advising her where to send the final paycheck.

***1057** In September of 2005, Holmes filed a lawsuit against defendants, asserting causes of action for sexual harassment, retaliation, wrongful termination in violation of public policy, violation of the right to privacy, and intentional infliction of emotional distress. She alleged that the negative comments in Petrovich's e-mails and his dissemination of her e-mails, which contained highly personal information, invaded her privacy, were intended to cause her great emotional distress, and caused her to quit her job to avoid the abusive and hostile work environment created by her employer. According to Holmes, Petrovich disseminated the e-mails to retaliate against her for inconveniencing him with her pregnancy and to cause her to quit. Holmes claimed she was constructively terminated in that continuing her employment with Petrovich "became untenable, as it would have been for any reasonable pregnant woman."

On November 17, 2006, defendants filed a motion for summary judgment or summary adjudication on the ground that, as a matter of law, Holmes could not establish any of her causes of action. Defendants argued Holmes could not establish (1) that there was an objectively or subjectively hostile work environment; (2) that she suffered an adverse employment action in retaliation for her pregnancy; (3) that she suffered an adverse employment action that would cause a reasonable person to quit; (4) that Holmes had a reasonable expectation of privacy in her e-mails; or (5) that Petrovich's conduct was extreme and outrageous.

The trial court granted the motion for summary adjudication as to three of the causes of action. The court ruled that, although there was evidence that Holmes subjectively perceived her workplace as hostile or abusive, there must also be evidence that the work environment was objectively offensive. "The undisputed brief, isolated, work-related exchanges between her and Mr. Petrovich, and others in the office, could not be objectively found to have been severe enough or sufficiently pervasive to alter the conditions of her employment and create a hostile or abusive work environment based upon her pregnancy." As for Holmes's claims for retaliation and constructive discharge, there was no evidence she experienced an adverse employment action, and no evidence****888** from which a reasonable trier of fact could find that Petrovich "intentionally created or knowingly permitted working conditions that were so intolerable or aggravated at the time of [Holmes's] resignation that a reasonable employer would realize that a reasonable person in [her] position would be compelled to resign."

The trial court denied the motion for summary adjudication as to the causes of action for invasion of privacy and intentional infliction of emotional dis-

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

tress. The court ruled that, despite Holmes's use of e-mail to communicate private information to Petrovich, and despite the company's policy regarding ***1058** the nonprivate nature of electronic communications, triable issues of fact remained regarding whether Petrovich's dissemination of the information to other people in the office breached Holmes's right to privacy or whether the disclosure was privileged, and that issues of fact remained concerning whether the disclosure was egregious and outrageous.

The trial of those two causes of action resulted in a defense verdict.

DISCUSSION

I

Holmes contends the trial court erred in granting defendants' motion for summary adjudication on her causes of action for sexual harassment, retaliation, and constructive discharge.

[1] A motion for summary judgment "shall be granted if all the papers submitted show that there is no triable issue as to any material fact and that the moving party is entitled to judgment as a matter of law." (Code Civ. Proc., § 437c, subd. (c).) Legal questions are considered de novo on appeal. (*Unisys Corp. v. California Life & Health Ins. Guarantee* Assn. (1998) 63 Cal.App.4th 634, 637, 74 Cal.Rptr.2d 106.) However, we must presume the judgment is correct, and the appellant bears the burden of demonstrating error. (*Howard v. Thrifty Drug & Discount Stores* (1995) 10 Cal.4th 424, 443, 41 Cal.Rptr.2d 362, 895 P.2d 469.)

Viewing Holmes's specific contentions within the context of the appropriate legal framework, we find no error.

A

First, Holmes contends the trial court erred in granting summary adjudication with respect to her cause of action for sexual harassment.

The Fair Employment and Housing Act (FEHA) makes it an unlawful employment practice for an employer, "because of ... sex, ... to harass an employee." (Gov.Code, § 12940, subd. (j)(1).) Under FEHA, " 'harassment' because of sex includes sexual harassment, gender harassment, and harassment based on pregnancy, childbirth, or related medical conditions." (Gov.Code, § 12940, subd. (j)(4)(C).)

[2] There are two theories upon which sexual harassment may be alleged: quid pro quo harassment, where a term of employment is conditioned upon ***1059** submission to unwelcome sexual advances, and hostile work environment, where the harassment is sufficiently pervasive so as to alter the conditions of employment and create an abusive work environment. (*Mogilefsky v. Superior Court* (1993) 20 Cal.App.4th 1409, 1414, 26 Cal.Rptr.2d 116.) Holmes pursued the latter.

[3] To prevail on a claim of hostile work environment sexual harassment, an employee must demonstrate that he or she was subjected to sexual advances, conduct, or comments that were (1) unwelcome, (2) because of sex, and (3) sufficiently severe or pervasive to alter the conditions of his ****889** or her employment and create an abusive work environment. (*Lyle v. Warner Brothers Television Productions* (2006) 38 Cal.4th 264, 279, 42 Cal.Rptr.3d 2, 132 P.3d 211 (hereafter *Lyle*).)

[4][5] " ' "[W]hether an environment is 'hostile' or 'abusive' can be determined only by looking at all the circumstances [including] the frequency of the discriminatory conduct; its severity; whether it is physically threatening or humiliating, or a mere offensive utterance; and whether it unreasonably interferes with an employee's work performance." [Citation.]' [Citation.] Therefore, to establish liability in a FEHA hostile work environment sexual harassment

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

case, a plaintiff employee must show she was subjected to sexual advances, conduct, or comments that were *severe enough or sufficiently pervasive to alter the conditions of her employment and create a hostile or abusive work environment.*" (*Lyle, supra,* 38 Cal.4th at p. 283, 42 Cal.Rptr.3d 2, 132 P.3d 211; original italics.) "With respect to the pervasiveness of harassment, courts have held an employee generally cannot recover for harassment that is occasional, isolated, sporadic, or trivial; rather, the employee must show a concerted pattern of harassment of a repeated, routine, or a generalized nature." (*Ibid.*)

[6] "To be actionable, 'a sexually objectionable environment must be both objectively and subjectively offensive, one that a reasonable person would find hostile or abusive, and one that the victim in fact did perceive to be so.' [Citations.] *That means a plaintiff who subjectively perceives the workplace as hostile or abusive will not prevail under the FEHA, if a reasonable person in the plaintiff's position, considering all the circumstances, would not share the same perception.* Likewise, a plaintiff who does not perceive the workplace as hostile or abusive will not prevail, even if it objectively is so." (*Lyle, supra,* 38 Cal.4th at p. 284, 42 Cal.Rptr.3d 2, 132 P.3d 211; italics added.)

Relying on *Lyle,* the trial court found that, although Holmes subjectively perceived her workplace as hostile, it was not an abusive environment from an objective standpoint as a matter of law. Holmes claims the trial court erred in relying on *Lyle* because the facts in that case are distinguishable. But the trial court did not grant Petrovich's motion based on a factual comparison to ***1060** *Lyle;* it simply used the standard of review established therein as it was required to do, and as are we, under principles of stare decisis. (*Auto Equity Sales, Inc. v. Superior Court of Santa Clara* (1962) 57 Cal.2d 450, 455, 20 Cal.Rptr. 321, 369 P.2d 937.)

Holmes contends the proper standard in sexual harassment cases is whether a reasonable woman would consider the work environment a hostile one and, hence, the standard in pregnancy discrimination cases should be whether a reasonable pregnant woman would consider her work environment hostile. Thus, Holmes asserts, "Unless there was undisputed evidence that [she] was an *unreasonable* pregnant woman, it is oxymoronic that the lower court found the conduct at issue subjectively offensive but not 'objectively' offensive to a reasonable pregnant woman in [her] position.... Quite frankly, the issue of 'objectively offensive conduct' should have been left to the trier of fact and not been a question of law for the judge to have decided, especially if it was clear that there was subjective offense and highly questionable conduct at issue." (Original italics.)

[7] Holmes's argument is not persuasive. An evaluation of all the circumstances surrounding Holmes's employment discloses an absence of evidence from which a reasonable jury could objectively ****890** find that Petrovich created a hostile work environment for a reasonable pregnant woman. During the two months Holmes worked for Petrovich, there was no severe misconduct or pervasive pattern of harassment. Holmes claims that her coworkers treated her differently based upon her pregnancy by asking about her maternity leave, but she admits that, when she asked them to stop, they complied.

Holmes points to the e-mails she exchanged with Petrovich on August 6 and 9, 2004, in which he implied she had deceived him about her pregnancy, stated he was offended that she had changed the period of time she would be absent for maternity leave, and asserted that her pregnancy was an extreme hardship on his business. She also complains that Petrovich unnecessarily forwarded to others her e-mail containing personal information about her age, prior miscarriages, and the possibility she would have terminated her pregnancy if the amniocentesis results

had revealed problems with the fetus. Holmes asserts that Petrovich did this to humiliate her. Petrovich said he sent the e-mails to in-house counsel and employees involved in human relations because he thought that Holmes was about to quit.

When viewed in context, the e-mails (set forth at length, *ante*) show nothing more than that Petrovich made some critical comments due to the stress of being a small business owner who must accommodate a pregnant woman's right to maternity leave. He recognized Holmes's legal rights, stated he would honor them, said he was not asking for her resignation, noted he ***1061** had been pleased with her work, and simply expressed his feelings as a "human in a tough business where people are constantly trying to take advantage of me." He assured Holmes that "it will work." Rather than giving him a chance to honor his promise, Holmes quit.

[8] It appears Holmes expects FEHA to be a civility code. It is not. (*Lyle, supra,* 38 Cal.4th at p. 295, 42 Cal.Rptr.3d 2, 132 P.3d 211.) As we stated above, there is no recovery for harassment that is occasional, isolated, sporadic, or trivial. (*Id.* at p. 283, 42 Cal.Rptr.3d 2, 132 P.3d 211.) Rather, a plaintiff must show a concerted pattern of harassment that is repeated, routine, or generalized in nature. (*Mokler v. County of Orange* (2007) 157 Cal.App.4th 121, 142, 68 Cal.Rptr.3d 568.) Holmes failed to do so. The isolated incidents to which she points are objectively insufficient.

Holmes relies on three cases for the proposition that harassment need not be pervasive and may be established by only a few instances of conduct over a short period of time. She fails to recognize that harassment need not be pervasive *if it is sufficiently severe* enough to alter the conditions of employment. (*Lyle, supra,* 38 Cal.4th at p. 283, 42 Cal.Rptr.3d 2, 132 P.3d 211 [the plaintiff must be subjected to conduct or comments severe enough *or* sufficiently pervasive to alter the conditions of her employment and create a hostile work environment].) The cases upon which Holmes relies are not remotely similar to her situation in that they all involve egregious and severe conduct that unquestionably was abusive. In *Hostetler v. Quality Dining, Inc.* (7th Cir.2000) 218 F.3d 798, the plaintiff's harasser engaged in three incidents over a one-week period of time: (1) he forced his tongue into her mouth, (2) he attempted to kiss her again and to remove her bra, and (3) he told her that he could perform oral sex so effectively he could make her do cartwheels. (*Id.* at pp. 802, 807–808.) In *Erdmann v. Tranquility Inc.* (N.D.Cal.2001) 155 F.Supp.2d 1152, a homosexual employee's boss insisted that the employee become heterosexual, convert to the employer's ****891** Mormon faith, and lead the company's prayer service. (*Id.* at pp. 1160–1161.) And in *Mayfield v. Trevors Store, Inc.* (N.D.Cal., Dec. 6, 2004, No. C–04–1483 MHP) 2004 WL 2806175, the employer not only made comments that made the plaintiff feel stigmatized due to her pregnancy, the employer also wrote negative performance evaluations, assigned the plaintiff large amounts of extra work, and denied her a sick day.

Petrovich did not engage in any similarly egregious conduct, and he provided a nondiscriminatory explanation for his conduct. Because Holmes produced no evidence from which a reasonable jury could infer the existence of a hostile work environment, the trial court correctly granted the motion for summary adjudication on this cause of action.

***1062** B

[9][10] Next, Holmes contends the court erred in granting the motion for summary adjudication on her cause of action for constructive discharge. According to Holmes, she "found the extreme stress associated with being out of work to be preferable to the treatment she was receiving at Petrovich." This claim fares no better than her last.

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

"Constructive discharge occurs only when the employer coerces the employee's resignation, either by creating working conditions that are intolerable under an objective standard, or by failing to remedy objectively intolerable working conditions that actually are known to the employer." (*Mullins v. Rockwell Internat. Corp.* (1997) 15 Cal.4th 731, 737 [63 Cal.Rptr.2d 636, 936 P.2d 1246].) The conditions prompting resignation must be "sufficiently extraordinary and egregious to overcome the normal motivation of a competent, diligent, and reasonable employee to remain on the job." (*Turner v. Anheuser–Busch, Inc.* (1994) 7 Cal.4th 1238, 1246 [32 Cal.Rptr.2d 223, 876 P.2d 1022], disapproved on other grounds by *Romano v. Rockwell Internat., Inc.* (1996) 14 Cal.4th 479 [59 Cal.Rptr.2d 20, 926 P.2d 1114].) The resignation must be coerced, not merely a rational option chosen by the employee. (*Id.* at p. 1247 [32 Cal.Rptr.2d 223, 876 P.2d 1022].)

From an objective standpoint, the trial court correctly granted summary adjudication. "Where a plaintiff fails to demonstrate the severe or pervasive harassment necessary to support a hostile work environment claim, it will be impossible for her to meet the higher standard of constructive discharge: conditions so intolerable that a reasonable person would leave the job." (*Brooks v. City of San Mateo* (9th Cir.2000) 229 F.3d 917, 930.) As discussed above, Holmes failed to present sufficient evidence of a hostile work environment. Thus, her wrongful termination claim necessarily fails. (*Jones v. Department of Corrections & Rehabilitation* (2007) 152 Cal.App.4th 1367, 1381, 62 Cal.Rptr.3d 200 (hereafter *Jones*).)

C

The trial court also granted summary adjudication on Holmes's cause of action for retaliation, ruling there was no evidence of an adverse employment action by Petrovich. We agree.

[11] Holmes argues that she was subjected to negative comments and accusations about her pregnancy, followed by Petrovich's retaliatory conduct when she told him she planned to exercise her leave rights—he retaliated by forwarding her sensitive personal information to others in the office, who had ***1063** no reason to know about her prior miscarriages, amniocentesis, and potential termination of her pregnancy.

****892** This is insufficient to establish an adverse employment action by Petrovich.

[12][13][14] An "adverse employment action," which is a critical component of a retaliation claim (*Jones, supra,* 152 Cal.App.4th at p. 1380, 62 Cal.Rptr.3d 200), requires a "substantial adverse change in the terms and conditions of the plaintiff's employment." (*Akers v. County of San Diego* (2002) 95 Cal.App.4th 1441, 1454, 1455, 116 Cal.Rptr.2d 602.) " '[A] mere offensive utterance or ... a pattern of social slights by either the employer or coemployees cannot properly be viewed as materially affecting the terms, conditions, or privileges of employment for purposes of [the FEHA]....' " (*Yanowitz v. L'Oreal USA, Inc.* (2005) 36 Cal.4th 1028, 1054, 32 Cal.Rptr.3d 436, 116 P.3d 1123 (hereafter *Yanowitz*).) "However, a series of alleged discriminatory acts must be considered collectively rather than individually in determining whether the overall employment action is adverse [citations] and, in the end, the determination of whether there was an adverse employment action is made on a case-by-case basis, in light of the objective evidence." (*Jones, supra,* 152 Cal.App.4th at p. 1381, 62 Cal.Rptr.3d 200.)

Here, Petrovich did not reduce Holmes's salary, benefits or work hours, and did not terminate her. He assured Holmes that she still had a job and that they would work things out. Holmes chose to quit because Petrovich expressed his concerns about the changes in her pregnancy leave dates and the need to replace her while she was on leave, and because he forwarded an

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

e-mail that she wished to keep private. But she failed to demonstrate there was a triable issue of fact concerning whether he did these things to retaliate against her; she simply concluded that this was his motivation by taking out of context certain comments that he made. Holmes overlooks her own evidence, submitted in opposition to defendants' motion, which demonstrated that Petrovich forwarded the e-mail only to people he believed needed to know that Holmes had changed the anticipated date of her pregnancy leave and that she might be quitting. The fact that he forwarded her entire e-mail, rather than editing it or drafting a new one, does not demonstrate any animus toward her, given there was no clear directive in her e-mail that she did not wish others to see it.

More importantly, "[m]inor or relatively trivial adverse actions or conduct by employers or fellow employees that, from an objective perspective, are reasonably likely to do no more than anger or upset an employee cannot properly be viewed as materially affecting the terms, conditions, or privileges of employment and are not actionable...." (*Yanowitz, supra,* 36 Cal.4th at p. 1054, 32 Cal.Rptr.3d 436, 116 P.3d 1123.) That is what occurred here. A reasonable person would have talked ***1064** to Petrovich, expressed dismay at his actions, given him an opportunity to explain or apologize, and waited to see if conditions changed after the air had cleared. Instead, Holmes chose to quit despite Petrovich's assurances that he wanted her to stay and that things would work out.

[15][16][17] For the reasons stated above, the trial court correctly granted defendants' motion for summary adjudication.[FN2]

> FN2. In her reply brief, Holmes says the court should have denied the motion for summary adjudication in its entirety because it was not timely served. This argument is forfeited because it is raised for the first time in her reply brief without a showing of good cause. (*Garcia v. McCutchen* (1997) 16 Cal.4th 469, 482, fn. 10, 66 Cal.Rptr.2d 319, 940 P.2d 906; *Reichardt v. Hoffman* (1997) 52 Cal.App.4th 754, 764–765, 60 Cal.Rptr.2d 770.) "Points raised for the first time in a reply brief will ordinarily not be considered, because such consideration would deprive the respondent of an opportunity to counter the argument." (*American Drug Stores, Inc. v. Stroh* (1992) 10 Cal.App.4th 1446, 1453, 13 Cal.Rptr.2d 432; *Reichardt v. Hoffman, supra,* 52 Cal.App.4th at pp. 764–765, 60 Cal.Rptr.2d 770.) In any event, in overruling Holmes's objection to the defect in service, the court did not err in ruling Holmes waived the defect by filing an opposition and appearing at the hearing on the motion. (*Carlton v. Quint* (2000) 77 Cal.App.4th 690, 696–698, 91 Cal.Rptr.2d 844.)

****893** II

Holmes's remaining claims of error all arise from an alleged violation of her attorney-client privilege.

She contends the trial court abused its discretion in (1) denying her motion demanding the return of privileged documents, (2) permitting the introduction of the documents at trial, and (3) giving a limiting instruction that undermined her cause of action for invasion of privacy. She argues that the cumulative prejudicial effect of these errors requires reversal of the judgment.

Her arguments are premised on various statutes governing the attorney-client privilege as follows:

Evidence Code section 954 states in relevant part: "Subject to Section 912 and except as otherwise provided in this article, the client, whether or not a party, has a privilege to refuse to disclose, and to prevent another from disclosing, a confidential communica-

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

tion between client and lawyer....” (Further section references are to the Evidence Code unless otherwise specified.)

Section 952 provides that a “confidential communication between client and lawyer” is “information transmitted between a client and his or her lawyer in the course of that relationship and in confidence by a means which, so far as the client is aware, discloses the information to no third persons ***1065** other than those who are present to further the interest of the client in the consultation or those to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted....” (§ 952.)

Section 917 states in relevant part: “(a) If a privilege is claimed on the ground that the matter sought to be disclosed is a communication made in confidence in the course of the lawyer-client ... relationship, the communication is presumed to have been made in confidence and the opponent of the claim of privilege has the burden of proof to establish that the communication was not confidential. [¶] (b) A communication ... does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication....”

Section 912, subdivision (a) provides that the right of any person to claim a lawyer-client privilege “is waived with respect to a communication protected by the privilege if any holder of the privilege, without coercion, has disclosed a significant part of the communication or has consented to disclosure made by anyone. Consent to disclosure is manifested by any statement or other conduct of the holder of the privilege indicating consent to the disclosure, including failure to claim the privilege in any proceeding in which the holder has the legal standing and opportunity to claim the privilege.”

With this statutory framework in mind, we turn to Holmes's specific contentions.

A

Holmes argues the trial court erred in denying her motion for discovery sanctions,****894** seeking return of the e-mails that she sent her attorney, Joanna Mendoza, using the company's computer. We disagree.

During a deposition, defense counsel questioned Holmes about her e-mail correspondence with her attorney. Mendoza objected on the ground of attorney-client privilege.

Mendoza then wrote to defense counsel, Kevin Iams, demanded the return of the e-mails, and said she would seek a protective order if he refused. Iams replied that Holmes made a knowing waiver of the privilege when she communicated with counsel on the company's e-mail system after being advised that her e-mails were not private. Nevertheless, Iams wrote, “I recognize that this is not an area in which the law is settled.... What I propose as a resolution is a stipulated protective order whereby I and my ***1066** clients will agree that we will not use the emails or facsimile copies in any deposition or court proceeding, unless we provide you written notice 45 days in advance. This will allow us further time to meet and confer, obtain a further protective order, or if necessary, to seek the court's intervention.”

Mendoza initially refused the proposed resolution, but then agreed. On May 15, 2006, Iams wrote a confirmation letter stating that Mendoza agreed to delay filing for a protective order pending a review of the “proposed protective order” that Iams would draft, wherein he would agree not to use the documents in any deposition or court proceeding without first giving Mendoza 45 days' written notice. The letter noted,

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

however, that "by entering into the protective order, neither side is waiving any arguments it may have regarding the appropriate use of the [e-mails]." Stating that his schedule that week was hectic, Iams said he would strive to have a draft of the protective order to Mendoza by the end of the week for her review.

Before Iams drafted the stipulated protective order, Attorney Robin Perkins substituted in as defendants' counsel. Thereafter, Perkins used the e-mails in support of defendants' motion for summary judgment.

Holmes demanded that defendants withdraw the e-mail evidence, in accord with their agreement not to use it without prior notice. She submitted a declaration objecting to use of the attorney-client e-mails, claiming they were privileged.

Responding that the parties had never agreed not to utilize the e-mails, and that no protective order had ever been executed, defendants objected to Holmes's declaration that the e-mails were privileged. In defendants' view, the declaration was improper lay opinion, and Holmes had waived the attorney-client privilege. They pointed out that Holmes's counsel specifically permitted defendants' counsel to ask questions concerning the e-mails, stating: "If the only extent of your questions are going to be about this e-mail exchange, *and you're not going to go into a follow-up meeting that was had or any other communications with her attorney,* and it's not going to be considered a waiver of any of *those communications,* then I have no problem with it." (Italics added.)

The trial court sustained defendants' objections and did not exclude the e-mail evidence.

Thereafter, Holmes sought discovery sanctions for defendants' failure to return the e-mails and for violating the agreement not to use them without affording Holmes prior notice.

Defendants opposed the motion on the grounds that the parties never reached a written stipulation; Holmes never filed a motion to compel, which ***1067** meant the ****895** court had never ordered Petrovich to return the documents; and the court had already found that the use of the e-mails did not violate the attorney-client privilege.

The court denied the motion for discovery sanctions, finding defendants had not engaged in any discovery abuse. It explained: "With respect to the e-mails that were submitted by defendants with the motion for summary judgment/adjudication, the Court found plaintiff had waived attorney-client privilege...."

[18] Holmes contests this ruling, asserting "no specific finding of waiver was made" in connection with the motion for summary judgment because defendants' objections to the claim of attorney-client privilege were made on multiple grounds, and the court merely sustained the objection without specifying the basis for its ruling. Thus, she argues, the court erred in relying on a nonexistent finding of waiver to deny the discovery sanctions motion.

Holmes overlooks that Judge Shelleyanne Chang presided over both the motion for summary judgment and/or adjudication and the motion for discovery sanctions. We presume that Judge Chang knew the basis for her own ruling sustaining defendants' objections in the first proceeding. Hence, Judge Chang did not err in relying on her prior determination that Holmes waived the attorney-client privilege. Furthermore, as we shall explain in the next section of the opinion, the e-mails were not privileged.

B

Holmes asserts the court erred in overruling her motion in limine to prevent defendants from introducing the aforementioned e-mails at trial to show Holmes did not suffer severe emotional distress, was

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

only frustrated and annoyed, and filed the action at the urging of her attorney.

The court ruled that Holmes's e-mails using defendants' company computer were not protected by the attorney-client privilege because they were not private.

Holmes argues that the court did not understand the proper application of section 917, and thus erred in allowing introduction of the e-mail evidence. According to Holmes, "the California Legislature has already deemed [the fact that a communication was made electronically] to be irrelevant in determining whether a communication is confidential and therefore privileged." However, it is Holmes, not the trial court, who misunderstands the proper application of section 917.

[19] ***1068** Although a communication between persons in an attorney-client relationship "does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication" (§ 917, subd. (b)), this does not mean that an electronic communication is privileged (1) when the electronic means used belongs to the defendant; (2) the defendant has advised the plaintiff that communications using electronic means are not private, may be monitored, and may be used only for business purposes; and (3) the plaintiff is aware of and agrees to these conditions. A communication under these circumstances is not a " 'confidential communication between client and lawyer' " within the meaning of section 952 because it is not transmitted "by a means which, so far as the client is aware, discloses the information to no third persons other than those who are present to further the interest of the client in the consultation...." (*Ibid.*)

****896** When Holmes e-mailed her attorney, she did not use her home computer to which some unknown persons involved in the delivery, facilitation, or storage may have access. Had she done so, that would have been a privileged communication unless Holmes allowed others to have access to her e-mails and disclosed their content. Instead, she used defendants' computer, after being expressly advised this was a means that was not private and was accessible by Petrovich, the very person about whom Holmes contacted her lawyer and whom Holmes sued. This is akin to consulting her attorney in one of defendants' conference rooms, in a loud voice, with the door open, yet unreasonably expecting that the conversation overheard by Petrovich would be privileged.

Holmes disagrees, but the decisions upon which she relies are of no assistance to her because they involve inapposite factual circumstances, such as Fourth Amendment searches and seizures by public or government employers (*Quon v. Arch Wireless Operating Co., Inc.* (9th Cir.2008) 529 F.3d 892 (hereafter *Quon*), reversed by *City of Ontario v. Quon* (2010) ––U.S. ––––, 130 S.Ct. 2619, 2633, 177 L.Ed.2d 216, 231; *Leventhal v. Knapek* (2d Cir.2001) 266 F.3d 64; *Convertino v. U.S. Dept. of Justice* (D.D.C.2009) 674 F.Supp.2d 97, 110), or the use of a personal web-based e-mail account accessed from an employer's computer where the use of such an account was not clearly covered by the company's policy and the e-mails contained a standard hallmark warning that the communications were personal, confidential, attorney-client communications. (*Stengart v. Loving Care Agency, Inc.* (2010) 201 N.J. 300, 990 A.2d 650, 659, 663–664.)

[20] The present case does not involve similar scenarios. Holmes used her employer's company e-mail account after being warned that it was to be used ***1069** only for company business, that e-mails were not private, and that the company would randomly and periodically monitor its technology resources to ensure compliance with the policy. (Cf.

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

Scott v. Beth Israel Med. Center, Inc. (2007) 17 Misc.3d 934, 847 N.Y.S.2d 436, 441–443 [despite a statute similar to section 917, an attorney-client privilege did not exist when a company computer was used to send e-mails, and the company's policy prohibited the personal use of e-mails, warned that they were not private, and stated that they could be monitored].) [FN3]

FN3. Section 917, subdivision (b) is derived from the statute at issue in *Scott v. Beth Israel Med. Center, Inc., supra,* 17 Misc.3d 934, 847 N.Y.S.2d 436, New York's Civil Practice Law and Rules, section 4548, which states: "No communication privileged under this article shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication." (Cal. Law Revision Com. com., reprinted at 29B, pt. 3A West's Ann. Evid.Code (2009 ed.) foll. § 917, p. 267.)

Holmes emphasizes that she believed her personal e-mail would be private because she utilized a private password to use the company computer and she deleted the e-mails after they were sent. However, her belief was unreasonable because she was warned that the company would monitor e-mail to ensure employees were complying with office policy not to use company computers for personal matters, and she was told that she had no expectation of privacy in any messages she sent via the company computer. Likewise, simply because she "held onto a copy of the fax," she had no expectation of privacy in documents she sent to her attorney using the company's facsimile machine, a technology resource that, she was told, would ****897** be monitored for compliance with company policy not to use it for personal matters.

According to Holmes, even though the company unequivocally informed her that employees who use the company's computers to send personal e-mail have "no right of privacy" in the information sent (because the company would periodically inspect all e-mail to ensure compliance with its policy against personal use of company computers), she nonetheless had a reasonable expectation that her personal e-mail to her attorney would be private because the " 'operational reality' was that there was no access or auditing of employee's computers." (Citing *Quon, supra,* 529 F.3d 892, reversed by *City of Ontario v. Quon, supra,* —— U.S. at p. ——, 130 S.Ct. at p. 2633, 177 L.Ed.2d at p. 231.)

In support of this contention, Holmes claims she "knew that her computer was password protected and that no one had asked for or knew her password, and the only person who had the ability to inspect the computers did not ever perform that task." This misrepresents the record in two respects. It is inaccurate to say only one person had the ability to monitor e-mail sent and received on company computers. The company's controller, who had an administrative password giving her access to all e-mail sent by employees ***1070** with private passwords, testified that the company's "IT person" as well as company owner Cheryl Petrovich also had such access to e-mail sent and received by company computers. And at no time during her testimony did Holmes claim she knew for a fact that, contrary to its stated policy, the company never actually monitored computer e-mail. She simply said that, to her knowledge, no one did so.

In any event, Holmes's reliance on *Quon* is misplaced. There, a police sergeant, Jeff Quon, sued his employer, the Ontario Police Department, claiming it violated his Fourth Amendment right to be free of unlawful government searches and seizures when it reviewed text messages that he sent on an employer-issued text pager. (*Quon, supra,* 529 F.3d at p. 895.) In holding that Quon had a reasonable expectation of

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

privacy in his text messages due to the operational realities of the workplace, the Ninth Circuit relied in large part on the plurality opinion in *O'Connor v. Ortega* (1987) 480 U.S. 709, 107 S.Ct. 1492, 94 L.Ed.2d 714 (hereafter *O'Connor*). (*Quon, supra,* 529 F.3d at pp. 903–904, 907.)

O'Connor held that the fact an employee works for the government does not negate the employee's Fourth Amendment right to be free of unreasonable governmental searches and seizures at work. (*O'Connor, supra,* 480 U.S. at pp. 715, 717, 107 S.Ct. at pp. 1496–1497, 1497–1498, 94 L.Ed.2d at pp. 721, 723.) But "[t]he operational realities of the workplace ... may make *some* employees' expectations of privacy unreasonable." (*Id.* at p. 717, 107 S.Ct. at pp. 1497–1498, 94 L.Ed.2d at p. 723.) For example, the existence of specific office policies, practices, and procedures may have an effect on public employees' expectations of privacy in their workplace. (*Ibid.*) "Given the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis." (*Id.* at p. 718, 107 S.Ct. at p. 1498, 94 L.Ed.2d at p. 723.)

Relying on *O'Connor,* the Ninth Circuit upheld the district court's determination that Quon had a reasonable expectation of privacy in his text messages because, despite a departmental policy that users of pagers had no right to privacy, the operational reality was that Quon was given an expressly conflicting message to the contrary by his supervisor. ****898**(*Quon, supra,* 529 F.3d at p. 907.) In addition to finding Quon had a reasonable expectation of privacy, the Ninth Circuit found the search was unreasonable in violation of the Fourth Amendment. (*Id.* at pp. 908–909.)

The United States Supreme Court reversed this decision on the ground the search was not unreasonable. (*City of Ontario v. Quon, supra,* —— U.S. at p. ——, 130 S.Ct. at pp. 2631–2634, 177 L.Ed.2d at pp. 229–231.) Before turning to that issue, it noted that the parties disputed whether Quon had a reasonable expectation of privacy with respect to his pager messages. ***1071**(*Id.* at p. ——, 130 S.Ct. at p. 2629, 177 L.Ed.2d at p. 226.) Opting not to resolve this issue or whether the *O'Connor* "operational reality" test was applicable, the court observed that it "must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." (*Id.* at p. ——, 130 S.Ct. at p. 2629, 177 L.Ed.2d at pp. 226–227.) "Even if the Court were certain that the *O'Connor* plurality's approach were the right one, the Court would have difficulty predicting how employees' privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable.... And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated." (*Id.* at p. ——, 130 S.Ct. at p. 2630, 177 L.Ed.2d at p. 227.)

[21] Here, we are not concerned with a potential Fourth Amendment violation because Holmes was not a government employee. And, even assuming the "operational reality" test applies, it is of no avail to Holmes because the company explicitly told employees that they did not have a right to privacy in personal e-mail sent by company computers, which e-mail the company could inspect at any time at its discretion, and the company never conveyed a conflicting policy. Absent a company communication to employees explicitly contradicting the company's warning to them that company computers are monitored to make sure employees are not using them to send personal e-mail, it is immaterial that the "operational reality" is the company does not actually do so.

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

Just as it is unreasonable to say a person has a legitimate expectation that he or she can exceed with absolute impunity a posted speed limit on a lonely public roadway simply because the roadway is seldom patrolled, it was unreasonable for Holmes to believe that her personal e-mail sent by company computer was private simply because, to her knowledge, the company had never enforced its computer monitoring policy.

In sum, "so far as [Holmes was] aware," within the meaning of section 952, the company computer was not a means by which to communicate in confidence any information to her attorney. The company's computer use policy made this clear, and Holmes had no legitimate reason to believe otherwise, regardless of whether the company actually monitored employee e-mail. Thus, when, with knowledge of her employer's computer monitoring policy, Holmes used a company computer to e-mail her attorney about an employment action against her boss, Petrovich, Holmes in effect knowingly disclosed this information to a third party, the company and thus Petrovich, who certainly was not involved in furthering Holmes's interests in her consultation with her attorney (§ 952) because Petrovich was the party she eventually sued.

****899 *1072** Hence, the trial court correctly ruled that the attorney-client communication was not privileged. (§ 952.)

C

[22] According to Holmes, the trial court erred when it gave the jury a protective admonishment about the attorney-client e-mails.

The court stated: "Jury, normally you may be shocked to see something like this on screen. However, I determined in proceedings prior to trial that this was not privileged information between an attorney and a client because it was communicated through company computers." When Holmes's attorney began to object, the court responded, "the jury needs to understand that we are not romping wholesale over the attorney/client privilege. And I don't want the jury to be offended by this type of correspondence."

After an unreported sidebar conference, the court stated: "I think I've made it clear to you [the jurors] why you're being permitted to see this kind of unusual correspondence, and the only reason you're able to see it is for the reasons I expressed earlier, namely that it was correspondence on a company computer, but that has nothing whatsoever to do with Miss Holmes' claim of privacy with respect to the pregnancy issues she communicated to Mr. Petrovich and her claims of emotional distress from that. [¶] So don't take my comments as any kind of indication how you should decide the merits of this case based upon this attorney/client communication. It's a very, very different issue. [¶] But I felt you should know why I'm permitting you to see this, because it's a very unusual kind of correspondence between a client and an attorney that normally juries would not see, but you're seeing it for that very limited purpose, but consider it only for the very limited purpose ... and don't attach any importance to it on the main claim of Miss Holmes against [Petrovich]."

Holmes argues the above-quoted comments undermined her invasion of privacy claim by more or less advising the jury she had no right to privacy in e-mails on a company computer. Not so.

The causes of action for invasion of privacy and intentional infliction of emotional distress were not premised on Petrovich accessing Holmes's attorney-client e-mails, but on his forwarding to her coworkers her private e-mails to him about her pregnancy. She claimed that this dissemination of intimate details concerning her pregnancy violated her right to privacy, that Petrovich's conduct was outrageous, and that it caused Holmes great emotional distress.

191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 201 Daily Journal D.A.R. 671
(Cite as: 191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878)

***1073** The court unambiguously advised the jury that Holmes's e-mails to her attorney were being introduced for a limited purpose, and the court's determination that they were not privileged because they were sent on a company computer had "nothing whatsoever to do with [her] claim of privacy" and her claims of emotional distress. Then, in response to jury questions during deliberations, the court advised the jury that an electronic data transmission may constitute an invasion of privacy if the elements of the tort are established by a preponderance of the evidence,[FN4] and that policies in an employer handbook could not supersede California law.

> FN4. The court instructed the jury earlier that, to establish her claim for invasion of privacy, Holmes had to prove the following five elements: (1) she had a reasonable expectation of privacy in precluding the dissemination or misuse of sensitive and confidential information under the circumstances; (2) Petrovich invaded her privacy by disseminating or misusing her sensitive or confidential information; (3) the conduct was a serious invasion of her privacy; (4) she was harmed; and (5) Petrovich's conduct was a substantial factor in causing her harm.

****900** Holmes points to nothing indicating that the court's comments were a misstatement of the evidence or law. Unlike *Lewis v. Bill Robertson & Sons, Inc.* (1984) 162 Cal.App.3d 650, 208 Cal.Rptr. 699, upon which Holmes relies, the court did not commit misconduct and engage in partisan advocacy by expressing strong opinions on the ultimate issue at trial (*id.* at pp. 656–657, 208 Cal.Rptr. 699), i.e., whether Petrovich invaded her right to privacy by forwarding to Holmes's coworkers the e-mails about her pregnancy. Under the circumstances, she has failed to meet her burden of establishing error. (*Badie v. Bank of America* (1998) 67 Cal.App.4th 779, 784–785, 79 Cal.Rptr.2d 273 [it is the appellants' burden to establish error with reasoned argument and citations to authority].)

[23] Holmes also fails to meet her burden of establishing that the alleged error was prejudicial. (*In re Marriage of McLaughlin* (2000) 82 Cal.App.4th 327, 337, 98 Cal.Rptr.2d 136 [an appellant bears the burden of establishing prejudice by spelling out in his or her brief exactly how an alleged error caused a miscarriage of justice]; *American Drug Stores, Inc. v. Stroh, supra,* 10 Cal.App.4th at p. 1453, 13 Cal.Rptr.2d 432 [appellants may not attempt to rectify their omissions and oversights for the first time in their reply briefs].) Holmes does not present a coherent argument explaining how the court's statement that her e-mails to her attorney were not privileged undermined her theory that Petrovich egregiously violated her privacy by forwarding e-mails about her difficult and sensitive pregnancy decisions to people she claimed had no legitimate business need to know about the matters discussed therein. Thus, Holmes fails to demonstrate that, but for the court's alleged errors, it is reasonably probable the jury would have returned a more favorable verdict. (*Cassim v. Allstate Ins. Co.* (2004) 33 Cal.4th 780, 801–802, 16 Cal.Rptr.3d 374, 94 P.3d 513.)

***1074** III

[24] In her reply brief, Holmes attempts to raise a new argument challenging the jury's verdict on her cause of action for invasion of privacy. The argument is entitled, "ONE DOES NOT LOSE THEIR [*sic*] CONSTITUTIONAL RIGHT TO PRIVACY SIMPLY BY WALKING THROUGH THE ENTRANCE OF THE WORKPLACE."

She asserts that an employer cannot destroy the constitutional right to privacy via a company handbook without due consideration being paid; that an employee has a reasonable expectation of privacy when an employer's technology policy is not enforced; and that an employer violates an employee's right to

privacy when he discloses private information about the employee without a legitimate business reason for doing so.

We decline to address this argument because it is raised for the first time in her reply brief and is thus forfeited. (*Garcia v. McCutchen, supra,* 16 Cal.4th at p. 482, fn. 10, 66 Cal.Rptr.2d 319, 940 P.2d 906; *Reichardt v. Hoffman, supra,* 52 Cal.App.4th at pp. 764–765, 60 Cal.Rptr.2d 770; *American Drug Stores, Inc. v. Stroh, supra,* 10 Cal.App.4th at p. 1453, 13 Cal.Rptr.2d 432.)

DISPOSITION

The judgment is affirmed.

We concur: HULL, Acting P.J., and BUTZ, J.

Cal.App. 3 Dist.,2011.
Holmes v. Petrovich Development Co.
191 Cal.App.4th 1047, 119 Cal.Rptr.3d 878, 111 Fair Empl.Prac.Cas. (BNA) 424, 11 Cal. Daily Op. Serv. 560, 2011 Daily Journal D.A.R. 671

END OF DOCUMENT

96 Cal.App.4th 443, 117 Cal.Rptr.2d 155, 18 IER Cases 545, 02 Cal. Daily Op. Serv. 1740, 2002 Daily Journal D.A.R 2091
(Cite as: 96 Cal.App.4th 443, 117 Cal.Rptr.2d 155)

Court of Appeal, Second District, Division 1, California.
TBG INSURANCE SERVICES CORPORATION, Petitioner,
v.
The SUPERIOR COURT of Los Angeles County, Respondent;
Robert Zieminski, Real Party in Interest.

No. B153400.
Feb. 22, 2002.
Rehearing Denied March 14, 2002.
Review Denied June 12, 2002.[FN*]

FN* Kennard, J., dissented.

During discovery in former employee's wrongful termination action against former employer, former employer brought motion to compel production of former employee's home computer, which former employer had provided for former employee. The Superior Court, Los Angeles County, No. BC246390,Alban I. Niles, J., denied the motion. Former employer petitioned for writ of mandate. The Court of Appeal, Miriam A. Vogel, J., held that: (1) home computer was relevant to issue of whether former employee's at-work access of sexually explicit web sites was voluntary; (2) waiver signed by former employee precluded any reasonable expectation of privacy in the computer; and (3) former employer's demand for production was not a serious invasion of former employee's privacy, notwithstanding the waiver.

Petition granted; writ issued.

West Headnotes

[1] Pretrial Procedure 307A 31

307A Pretrial Procedure
307AII Depositions and Discovery
307AII(A) Discovery in General
307Ak31 k. Relevancy and materiality. Most Cited Cases

Pretrial Procedure 307A 32

307A Pretrial Procedure
307AII Depositions and Discovery
307AII(A) Discovery in General
307Ak32 k. Probable admissibility at trial. Most Cited Cases

In the context of discovery, evidence is “relevant” if it might reasonably assist a party in evaluating its case, preparing for trial, or facilitating a settlement; admissibility is not the test, and it is sufficient if the information sought might reasonably lead to other, admissible evidence. West's Ann.Cal.C.C.P. § 2017(a).

[2] Pretrial Procedure 307A 407

307A Pretrial Procedure
307AII Depositions and Discovery
307AII(E) Production of Documents and Things and Entry on Land
307AII(E)4 Proceedings
307Ak404 Affidavits and Showing
307Ak407 k. Relevancy and materiality. Most Cited Cases

In the context of a demand for production of a

tangible thing during discovery, the party who asks the trial court to compel production must show good cause for the request, but unless there is a legitimate privilege issue or claim of attorney work product, that burden is met simply by a fact-specific showing of relevance. West's Ann.Cal.C.C.P. § 2031(a)(1, 2).

[3] Pretrial Procedure 307A 390

307A Pretrial Procedure
307AII Depositions and Discovery
307AII(E) Production of Documents and Things and Entry on Land
307AII(E)3 Particular Documents or Things
307Ak390 k. Objects and tangible things; entry on land. Most Cited Cases

Former employee's home computer was relevant to wrongful termination action against former employee, which allegedly terminated former employer in part for voluntary access of sexually explicit web-sites; former employee alleged that sexually explicit web-sites involuntarily popped up on his computer screen at work, and former employer wished to discover by examining his home computer whether former employer voluntarily accessed those same web sites at home so as to impeach claim that at-work access was accidental. West's Ann.Cal.C.C.P. § 2031(a)(1, 2).

[4] Civil Rights 78 1040

78 Civil Rights
78I Rights Protected and Discrimination Prohibited in General
78k1040 k. Privacy. Most Cited Cases
(Formerly 78k448.1)

When affirmative relief is sought to prevent a constitutionally prohibited invasion of privacy, the plaintiff must establish (1) a legally protected privacy interest, (2) a reasonable expectation of privacy in the circumstances, and (3) conduct by defendant constituting a serious invasion of privacy. West's Ann.Cal. Const. Art. 1, § 1.

[5] Constitutional Law 92 1215

92 Constitutional Law
92XI Right to Privacy
92XI(A) In General
92k1215 k. Reasonable, justifiable, or legitimate expectation. Most Cited Cases
(Formerly 92k82(7))

Assuming the existence of a legally cognizable privacy interest, the extent of that interest is not independent of the circumstances, and other factors, including advance notice, may affect a person's reasonable expectation of privacy. West's Ann.Cal. Const. Art. 1, § 1.

[6] Constitutional Law 92 1215

92 Constitutional Law
92XI Right to Privacy
92XI(A) In General
92k1215 k. Reasonable, justifiable, or legitimate expectation. Most Cited Cases
(Formerly 92k82(7))

A reasonable expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms, and the presence or absence of opportunities to consent voluntarily to activities impacting privacy interests obviously affects the expectations of the participant. West's Ann.Cal. Const. Art. 1, § 1.

[7] Constitutional Law 92 1212

92 Constitutional Law

96 Cal.App.4th 443, 117 Cal.Rptr.2d 155, 18 IER Cases 545, 02 Cal. Daily Op. Serv. 1740, 2002 Daily Journal D.A.R 2091

(Cite as: 96 Cal.App.4th 443, 117 Cal.Rptr.2d 155)

92XI Right to Privacy
92XI(A) In General
92k1212 k. Disclosure of personal matters. Most Cited Cases
(Formerly 92k82(7))

Constitutional Law 92 1213

92 Constitutional Law
92XI Right to Privacy
92XI(A) In General
92k1213 k. Making of personal decisions. Most Cited Cases
(Formerly 92k82(7))

There are two general classes of legally recognized privacy interests: (1) interests in precluding dissemination or misuse of sensitive and confidential information or "informational privacy," and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference or "autonomy privacy." West's Ann.Cal. Const. Art. 1, § 1.

[8] Constitutional Law 92 1215

92 Constitutional Law
92XI Right to Privacy
92XI(A) In General
92k1215 k. Reasonable, justifiable, or legitimate expectation. Most Cited Cases
(Formerly 92k82(7))

Torts 379 330

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)1 Privacy in General
379k330 k. In general. Most Cited Cases
(Formerly 379k8.5(2))

The community norms aspect of the reasonable expectation element of an invasion of privacy claim is this: the protection afforded to the plaintiff's interest in his privacy must be relative to the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbors and fellow citizens. West's Ann.Cal. Const. Art. 1, § 1.

[9] Searches and Seizures 349 26

349 Searches and Seizures
349I In General
349k25 Persons, Places and Things Protected
349k26 k. Expectation of privacy. Most Cited Cases

The use of computers in the employment context carries with it social norms that effectively diminish the employee's reasonable expectation of privacy with regard to his use of his employer's computers. West's Ann.Cal. Const. Art. 1, § 1.

[10] Constitutional Law 92 1229

92 Constitutional Law
92XI Right to Privacy
92XI(B) Particular Issues and Applications
92k1227 Records or Information
92k1229 k. Discovery. Most Cited Cases
(Formerly 92k82(7))

Pretrial Procedure 307A 390

307A Pretrial Procedure
307AII Depositions and Discovery
307AII(E) Production of Documents and Things and Entry on Land
307AII(E)3 Particular Documents or Things
307Ak390 k. Objects and tangible

things; entry on land. Most Cited Cases

Former employee, who agreed in writing that former employer could monitor home computer which it had provided for former employee's home use, did not have a reasonable expectation of privacy in the computer and thus could be compelled to produce the computer for discovery in wrongful termination action, despite alleged existence of personal material on the computer; former employee had the opportunity to consent to the policy or not, and could have limited computer use to purely business matters and purchased his own computer for personal use. West's Ann.Cal. Const. Art. 1, § 1; West's Ann.Cal.C.C.P. § 2031.

[11] Constitutional Law 92 1229

92 Constitutional Law
92XI Right to Privacy
92XI(B) Particular Issues and Applications
92k1227 Records or Information
92k1229 k. Discovery. Most Cited Cases
(Formerly 92k82(7))

Pretrial Procedure 307A 390

307A Pretrial Procedure
307AII Depositions and Discovery
307AII(E) Production of Documents and Things and Entry on Land
307AII(E)3 Particular Documents or Things
307Ak390 k. Objects and tangible things; entry on land. Most Cited Cases

Former employer's demand to former employee to produce during discovery in wrongful termination action a computer which former employer provided for former employee's use at his home was not a serious invasion of former employee's privacy so as to deny the right to compel production; appropriate protective orders could define the scope of inspection and copying of information on the computer to that directly relevant to the litigation, and could prohibit unnecessary copying and dissemination of former employee's financial and other information that had no rational bearing on the case. West's Ann.Cal. Const. Art. 1, § 1; West's Ann.Cal.C.C.P. § 2031.

****157 *445** Paul, Hastings, Janofsky & Walker, Eve M. Coddon and Bradley S. Pauley, Los Angeles, for Petitioner.

Astor & Phillips, Gary R. Phillips, George R. Phillips, Jr., and Ronald N. Sarian, Los Angeles, for Real Party in Interest.

No appearance for Respondent.

MIRIAM A. VOGEL, J.

An employer provided two computers for an employee's use, one for the office, the other to permit the employee to work at home. The employee, who had signed his employer's "electronic and telephone equipment policy statement" and agreed in writing that his computers could be monitored by his employer, was terminated for misuse of his office computer. After the employee sued the employer for wrongful termination, the employer demanded production of the home computer. The employee refused to produce the computer and the trial court refused to compel production. On the employer's petition, we conclude that, given the employee's consent to his employer's monitoring of both computers, the employee had no reasonable expectation of privacy when he used the home computer for personal matters. We issue the writ as prayed.

FACTS

For about 12 years, Robert Zieminski worked as a senior executive for TBG Insurance Services Corporation. In the course of his employment, ***446** Zie-

minski used two computers owned by TBG, one at the office, the other at his residence. Zieminski signed TBG's "electronic and telephone equipment policy statement" in which he agreed, among other things, that he would use the computers "for business purposes only and not for personal benefit or non-Company purposes, unless such use [was] expressly approved. Under no circumstances [could the] equipment or systems be used for improper, derogatory, defamatory, obscene or other inappropriate purposes." Zieminski consented to have his computer "use monitored by authorized company personnel" on an "as needed" basis, and agreed that communications transmitted by computer were not private. He acknowledged his understanding that his improper use of the computers could result in disciplinary action, including discharge.

In December 1998, Zieminski and TBG entered a "Shareholder Buy Sell Agreement," pursuant to which TBG sold 4,000 shares of its stock to Zieminski at $.01 per share; one-third of the stock was to vest on December 1, 1999, one-third on December 1, 2000, and one-third on December 1, ****158** 2001, each vesting contingent upon Zieminski's continued employment; if Zieminski's employment terminated before all of the shares had vested, TBG had the right to repurchase the non-vested shares at $.01 per share. As part of the buy-sell transaction, Zieminski signed a confidentiality agreement and gave TBG a two-year covenant not to compete. One-third of Zieminski's shares vested on December 1, 1999. In March 2000, TBG's shareholders (including Zieminski) sold a portion of their TBG shares to Nationwide Insurance Companies; more specifically, Zieminski sold 1,230 of his 1,333 vested shares to Nationwide for a cash price of $1,278,247.

On November 28, 2000, three days before another 1,333 shares were to vest, Zieminski's employment was terminated. According to TBG, Zieminski was terminated when TBG discovered that he "had violated TBG's electronic policies by repeatedly accessing pornographic sites on the Internet while he was at work." According to Zieminski, the pornographic Web sites were not accessed intentionally but simply "popped up" on his computer. Zieminski sued TBG, alleging that his employment had been wrongfully terminated "as a pretext to prevent his substantial stock holdings in TBG from fully vesting and to allow ... TBG to repurchase [his] non-vested stock" at $.01 per share.

TBG answered and (through its lawyers) asked Zieminski (through his lawyer) to return the home computer and cautioned Zieminski not to delete any information stored on the computer's hard drive. In response, Zieminski acknowledged that the computer was purchased by TBG and said he would either return it or purchase it, but said it would be necessary "to delete, alter, ***447** and flush or destroy some of the information on the computer's hard drive, since it contains personal information which is subject to a right of privacy." TBG refused to sell the computer to Zieminski, demanded its return without any deletions or alterations, and served on Zieminski a demand for production of the computer. (Code Civ. Proc., § 2031.) [FN1] Zieminski objected, claiming an invasion of his constitutional right to privacy.

FN1. All section references are to the Code of Civil Procedure.

TBG moved to compel production of the home computer, contending it has the right to discover whether information on the hard drive proves that, as claimed by TBG, Zieminski violated his employer's policy statement. In TBG's words, Zieminski's "repeated voluntary and non-work-related access of sexually explicit web-sites is ... one of the foremost issues in the case. As such, a significant piece of evidence in this action is the [home computer], as its hard drive may confirm that [Zieminski] has, in fact, accessed the same or similar sexually explicit web-sites

at home, thereby undermining [Zieminski's] ... story that, at work, such sites 'popped up' involuntarily." TBG suggested that, in light of Zieminski's agreement to be bound by TBG's policy statement, and in light of the fact that the home computer belongs to TBG, Zieminski could not seriously claim that he had a reasonable expectation of privacy when he used it for personal matters.

Zieminski opposed the motion, accused TBG of pursuing a " 'scorched earth' defense policy," demanded sanctions, and insisted that (notwithstanding the policy statement) he retained an expectation of privacy with regard to his home computer. According to Zieminski, the home computer was provided as a "perk" given to all senior executives. He said that, "[a]lthough the home computer was provided so that business related work could be done at home, it was universally accepted ****159** and understood by all that the home computers would also be used for personal purposes as well." He said his home computer was used by his wife and children, and that it "was primarily used for personal purposes and contains significant personal information and data" subject to his constitutional right of privacy (including "the details of [his] personal finances, [his] income tax returns," and all of his family's personal correspondence). Zieminski (who had admitted at his earlier deposition that he had signed the policy statement) did not mention the policy statement in his opposition memorandum or his declaration.[FN2]

> FN2. Zieminski's papers filed in opposition to TBG's writ petition are similarly silent on the subject of TBG's policy statement and his acceptance of it. Instead, Zieminski tells us, apropos of nothing, that we "should note" that in June of last year, a Marin County superior court judge overruled a demurrer in a class action alleging that the defendant's "practice of obtaining individuals' web browsing habits violated California consumers' right to privacy under the California Constitution." Leaving to one side the impropriety of Zieminski's citation of an unpublished and unpublishable superior court order (Cal. Rules of Court, rules 976, 977), the case is inapposite—because the alleged invasion of privacy arises out of the "secret accumulation of ... private information by an entity with whom [the plaintiffs] have not agreed to deal with...." (See *In re Doubleclick Cases* (Super. Ct. Marin County, 2001, No. JC4120) 2001 WL 1029646.) As we will explain, Zieminski's consent defeats his claim that he had a reasonable expectation of privacy.

The trial court denied TBG's motion, finding the information on the computer was "merely corroborative of facts already in [TBG's] possession;***448** since [TBG] already has extensive evidence, any additional evidence that the [home computer] may disclose does not outweigh the fact that the computer contains personal information." TBG then filed a petition for a writ of mandate, asking us to intervene. We issued an order to show cause and set the matter for hearing.

DISCUSSION

TBG contends it is entitled to inspect Zieminski's home computer. We agree.

A.

[1][2] A "party may obtain discovery regarding any matter, not privileged, that is relevant to the subject matter involved in the pending action ... if the matter either is itself admissible in evidence or appears reasonably calculated to lead to the discovery of admissible evidence." (§ 2017, subd. (a).) "In the context of discovery, evidence is 'relevant' if it might reasonably assist a party in evaluating its case, preparing for trial, or facilitating a settlement. Admissibility is *not* the test, and it is sufficient if the information sought might reasonably lead to other, admissible

evidence." (*Glenfed Development Corp. v. Superior Court* (1997) 53 Cal.App.4th 1113, 1117, 62 Cal.Rptr.2d 195.) In the more specific context of a demand for production of a tangible thing, the party who asks the trial court to compel production must show "good cause" for the request—but unless there is a legitimate privilege issue or claim of attorney work product, that burden is met simply by a fact-specific showing of relevance. (§ 2031, subds. (a)(2), (*l*); cf. *Glenfed Development Corp. v. Superior Court*, *supra*, 53 Cal.App.4th at p. 1117, 62 Cal.Rptr.2d 195.)

[3] Here, the home computer is indisputably relevant (Zieminski does not seriously contend otherwise),[FN3] and the trial ****160** court's finding that TBG already has other "extensive evidence" misses the mark. TBG is entitled to discover any non-privileged information, cumulative or not, that may reasonably assist it in evaluating its defense, preparing for trial, or facilitating a ***449** settlement. Admissibility is *not* the test, and it is sufficient if the information sought might reasonably lead to other, admissible evidence.[FN4] (*Irvington–Moore, Inc. v. Superior Court* (1993) 14 Cal.App.4th 733, 738–739, 18 Cal.Rptr.2d 49[a party may use multiple methods to obtain discovery and the fact that information was disclosed under one method is not, by itself, a proper basis to refuse to provide discovery under another method].) Zieminski offers no authority to the contrary, and we know of none. The issue, therefore, is whether he has a protectible privacy interest in the information to be found on the computer.

FN3. TBG contends "the history of Zieminski's Internet use stored on [his home computer's] hard drive, including the length of time spent at particular web-sites, [would] constitute unique and accurate evidence that Zieminski's access of improper non-business and sexually explicit web-sites at work was intentional, not accidental, as Zieminski contends," and that sexually explicit web-sites, if found on Zieminski's home computer, would impeach Zieminski's claim that these sites just "popped up" on his office computer. We agree that, if found on the home computer, this information would be relevant.

FN4. If admissibility mattered, the fact that TBG may have other evidence in its possession is immaterial. There has been no finding that any particular piece of evidence will be admissible, and there is no reason to make such a finding at this stage of the proceedings.

B.

[4] Zieminski's privacy claim is based on article I, section I, of the California Constitution, which provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." When affirmative relief is sought to prevent a constitutionally prohibited invasion of privacy, the plaintiff must establish "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." (*Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 39–40, 26 Cal.Rptr.2d 834, 865 P.2d 633.) Here, we assume the existence of an abstract privacy interest in Zieminski's financial and other personal information but conclude, by the reasons explained below, that the evidence is insufficient to support the trial court's implied finding that Zieminski had a reasonable expectation of privacy in the circumstances. As we also explain, the trial court may in any event make such orders as are necessary to minimize TBG's intrusion.

1.

[5][6][7] Assuming the existence of a legally

cognizable privacy interest, the extent of that interest is not independent of the circumstances, and other factors (including advance notice) may affect a person's reasonable expectation of privacy. (*Hill v. National Collegiate Athletic Assn., supra,* 7 Cal.4th at p. 36, 26 Cal.Rptr.2d 834, 865 P.2d 633.) "A 'reasonable' expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms," and "the presence or absence of opportunities to consent voluntarily to activities impacting privacy interests obviously affects the expectations of the participant." ***450**(*Id.* at p. 37, 26 Cal.Rptr.2d 834, 865 P.2d 633.) [FN5] ****161** Accordingly, our decision about the reasonableness of Zieminski's claimed expectation of privacy must take into account any "accepted community norms," advance notice to Zieminski about TBG's policy statement, and whether Zieminski had the opportunity to consent to or reject the very thing that constitutes the invasion. (*Id.* at pp. 36, 42, 26 Cal.Rptr.2d 834, 865 P.2d 633.)

FN5. Although *Hill* suggests that consent is a complete defense to a constitutional privacy claim (*Hill v. National Collegiate Athletic Assn., supra,* 7 Cal.4th at p. 40, 26 Cal.Rptr.2d 834, 865 P.2d 633), at least one court of appeal has viewed consent "as a factor in the balancing analysis, and not as a complete defense to a privacy claim." (*Kraslawsky v. Upper Deck Co.* (1997) 56 Cal.App.4th 179, 193, 65 Cal.Rptr.2d 297; see also Chin, Cathcart, Aexelrod & Wiseman, Cal. Practice Guide: Employment Litigation (The Rutter Group 2001) ¶ 5:731, p. 5–62.) In the drug testing cases, including *Hill* and *Kraslawsky,* the invasion of privacy is far more substantial than in our case. As the Supreme Court explained in *Hill,* there are two general classes of legally recognized privacy interests: (1) interests in precluding dissemination or misuse of sensitive and confidential information or "informational privacy"; and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference or "autonomy privacy." (*Hill v. National Collegiate Athletic Assn., supra,* 7 Cal.4th at p. 35, 26 Cal.Rptr.2d 834, 865 P.2d 633.) There is another significant distinction between the drug cases and our case. When an employer requires drug testing as a condition of employment, the employee must either submit to the invasion of his "autonomy privacy" or, typically, lose his job. When an employer requires consent to computer monitoring, the employee may have his cake and eat it too—he can avoid any invasion of his privacy by using his computer for business purposes only, and not for anything personal. In the context of the case before us, we view Zieminski's consent as a complete defense to his invasion of privacy claim. With consent viewed as one of several factors, we would reach the same result—because the invasion is slight and the need for disclosure great.

(a)

[8] The "community norms" aspect of the "reasonable expectation" element of an invasion of privacy claim is this: " 'The protection afforded to the plaintiff's interest in his privacy must be relative to the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbors and fellow citizens.' " (*Hill v. National Collegiate Athletic Assn., supra,* 7 Cal.4th at p. 37, 26 Cal.Rptr.2d 834, 865 P.2d 633, quoting Rest.2d, Torts, § 652D, com. c.) In *Hill,* where the issue was whether drug testing constituted an invasion of privacy, the "community" was "intercollegiate athletics, particularly in highly competitive postseason championship events," which by their nature involve "close regulation and scrutiny of the physical fitness and bodily condition of student athletes. Required physical examinations (including urinalysis), and special regulation of sleep habits, diet,

fitness, and other activities that intrude significantly on privacy interests are routine aspects of a college athlete's life not shared by other students or the population at large.... [¶] As a result of its unique set of demands, athletic participation carries with it social norms that effectively diminish the athlete's reasonable expectation of ***451** personal privacy in his or her bodily condition, both internal and external." (*Hill v. National Collegiate Athletic Assn., supra,* 7 Cal.4th at pp. 41–42, 26 Cal.Rptr.2d 834, 865 P.2d 633.)[FN6]

FN6. At the time *Hill* was decided, the Supreme Court recognized that, like "other claims for invasion of the state constitutional right to privacy, future [drug testing] claims arising in the employment context will be subject to the elements and standards [the high court announced in *Hill*], which require careful consideration of reasonable expectations of privacy and employer, employee, and public interests arising in particular circumstances." (*Hill v. National Collegiate Athletic Assn., supra,* 7 Cal.4th at pp. 55–56, fn. 20, 26 Cal.Rptr.2d 834, 865 P.2d 633.)

We are concerned in this case with the "community norm" within 21st Century computer-dependent businesses. In 2001, the 700,000 member American Management****162** Association (AMA) reported that more than three-quarters of this country's major firms monitor, record, and review employee communications and activities on the job, including their telephone calls, e-mails, Internet connections, and computer files. Companies that engage in these practices do so for several reasons, including legal compliance (in regulated industries, such as telemarketing, to show compliance, and in other industries to satisfy "due diligence" requirements), legal liability (because employees unwittingly exposed to offensive material on a colleague's computer may sue the employer for allowing a hostile workplace environment), performance review, productivity measures, and security concerns (protection of trade secrets and other confidential information). (American Management Assn., 2001 AMA Survey, Workplace Monitoring & Surveillance, Summary of Key Findings (April 2001) (hereafter "AMA Findings") <http//:www.amanet.org/research> [as of Feb. 13, 2002]; and see McIntosh, *E–Monitoring@Workplace.com: The Future of Communication Privacy in the Minnesota Private–Sector Workplace,* 23 Hamline L.Rev. 539, 541–542, fn. 10.)

[9] It is hardly surprising, therefore, that employers are told they "should establish a policy for the use of [e-mail and the Internet], which every employee should have to read and sign. First, employers can diminish an individual employee's expectation of privacy by clearly stating in the policy that electronic communications are to be used solely for company business, and that the company reserves the right to monitor or access all employee Internet or e-mail usage. The policy should further emphasize that the company will keep copies of Internet or e-mail passwords, and that the existence of such passwords is not an assurance of the confidentiality of the communications. [¶] An electronic communications policy should include a statement prohibiting the transmission of any discriminatory, offensive or unprofessional messages. Employers should also inform employees that access to any Internet sites that are discriminatory or offensive is not allowed, and no employee should be permitted to post personal opinions on the Internet using the company's access, particularly if the opinion is of a ***452** political or discriminatory nature." (Fernandez, *Workplace Claims: Guiding Employers and Employees Safely In And Out of the Revolving Door* (1999) 614 Practising Law Institute, Litigation and Administrative Practice Course Handbook Series, Litigation 725; see also Gantt, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace* (Spring 1995) 8 Harv. J.L. & Tech. 345, 404–405 [numerous commentators recommend that employers establish

corporate policies addressing e-mail privacy, and many employers have done just that].) [FN7] For these reasons, the use of computers in the employment context carries with it social norms that effectively diminish the employee's reasonable expectation of privacy with regard to his use of his employer's computers. (Cf. ****163***Hill v. National Collegiate Athletic Assn., supra*, 7 Cal.4th at p. 42, 26 Cal.Rptr.2d 834, 865 P.2d 633.) [FN8]

FN7. There can be serious consequences for inattentive employers. (E.g., *Cotran v. Rollins Hudig Hall Internat., Inc.* (1998) 17 Cal.4th 93, 69 Cal.Rptr.2d 900, 948 P.2d 412; *Curtis v. Citibank, N.A.* (2d Cir.2000) 226 F.3d 133; *Owens v. Morgan Stanley & Co.* (S.D.N.Y.1997) 1997 WL 403454, 74 Fair Empl. Prac. Cas. (BNA) 876; and see Settle Vinson, *Employer Liability for Messages Sent by Employees Via EMail and Voice Mail Systems* (1998) 24 T. Marshall L.Rev. 55.)

FN8. According to the AMA Findings, four out of ten surveyed companies allow employees full and unrestricted use of office e-mail, but "only one in ten allow the same unrestricted access to the internet. Companies are far more concerned with keeping explicit sexual content off their employees' screens than with any other content or matter." (AMA Findings, *supra*, <http//:www.amanet.org/research>.) See also, *Com. v. Proetto* (2001) 771 A.2d 823, 829, 832 [any reasonably intelligent person "savvy enough" to use the Internet is aware that messages are received in a recorded format and can be downloaded or printed by the party receiving the message; by sending a communication over the Internet, the party expressly consents to the recording of the message and demonstrates that he has "no reasonable expectation of privacy in his e-mails"]; *Bohach v. City of Reno* (D.Nev.1996) 932 F.Supp. 1232; (compare Gantt, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace, supra*, 8 Harv. J.L. & Tech. 345.)

(b)

[10] TBG's advance notice to Zieminski (the company's policy statement) gave Zieminski the opportunity to consent to or reject the very thing that he now complains about, and that notice, combined with his written consent to the policy, defeats his claim that he had a reasonable expectation of privacy. [FN9]

FN9. According to the AMA Findings, "[t]here is a strong correlation between active monitoring practices and formal, written policies covering e-mail, internet, and/or software use. Ninety-five percent of companies that actively monitor employees have written policies, compared with 75% of those that do no monitoring." (AMA Findings, *supra*, <http//: www.amanet.org/ research>.)

Several months after Zieminski started using the home computer, he signed TBG's policy statement, thereby acknowledging his understanding that the home computer was "the property of the Company" and, as such, "to be used for business purposes only and not for personal benefit or non-Company purposes." He agreed that the computer would not "be used for ***453** improper, derogatory, defamatory, obscene or other inappropriate purposes," acknowledged his understanding that "communications transmitted by Company systems [were] not considered private," and consented to TBG's designation of "authorized personnel to enter such systems and monitor messages and files on an 'as needed' basis." He was notified that this monitoring could "include the review, copying or deletion of messages, or the disclosure of such messages or files to other authorized persons." His sig-

nature shows that he read TBG's policy, understood it, and agreed to adhere to it.

As can be seen, Zieminski knew that TBG would monitor the files and messages stored on the computers he used at the office and at home. He had the opportunity to consent to TBG's policy or not, and had the opportunity to limit his use of his home computer to purely business matters. To state the obvious, no one compelled Zieminski or his wife or children to use the home computer for personal matters, and no one prevented him from purchasing his own computer for his personal use. With all the information he needed to make an intelligent decision, Zieminski agreed to TBG's policy *and* chose to use his computer for personal matters. By any reasonable standard, Zieminski fully and voluntarily relinquished his privacy rights in the information he stored on his home computer, and he will not now be heard to say that he nevertheless had a *reasonable* expectation of privacy. (*Hill v. National Collegiate Athletic Assn., supra,* 7 Cal.4th at pp. 36, 42, 26 Cal.Rptr.2d 834, 865 P.2d 633; see also *Feminist Women's Health Center v. Superior Court* (1997) 52 Cal.App.4th 1234, 1247–1249, 61 Cal.Rptr.2d 187 [where an employer is not ****164** obligated to hire a particular employee, the employee's consent to even a serious privacy invasion defeats the employee's claim that she had a reasonable expectation of privacy].)

In his declaration filed in opposition to TBG's motion to compel production of the home computer, Zieminski states that "it was universally accepted and understood by all [senior executives at TBG] that the home computers would also be used for personal purposes," and that he was never "informed that [he] could not use the home computer for personal purposes, or that [he] should not have an expectation of privacy with respect to the personal contents." His declaration is conveniently silent about the signed TBG policy statement, and about his admission (at his earlier deposition) that he had in fact signed the policy statement, and his self-serving hearsay statements are not corroborated by other TBG employees or by anyone. Under these circumstances, Zieminski's declaration cannot be viewed as substantial evidence of anything. (Cf. *D'Amico v. Board of Medical Examiners* (1974) 11 Cal.3d 1, 21–22, 112 Cal.Rptr. 786, 520 P.2d 10 [where an admission or concession is obtained not in the normal course of human activities but in ***454** the context of an established pretrial procedure whose purpose is to elicit facts, and where such an admission becomes relevant to the determination whether there exists an issue of *fact*, the admission trumps a subsequent declaration to the contrary].)[FN10]

FN10. We summarily reject Zieminski's assertions (1) that, simply by reason of the computer's use at his home, his "right of privacy is at its zenith," and (2) that his family's use of his company-owned computer somehow imbues the information stored on the computer with an aura of privacy that otherwise would not exist. We agree with TBG that, in "today's portable society, where one's computer files can be held and transported in the palm of the hand, relevant evidence should not escape detection solely because it was created within the physical confines of one's home."

2.

[11] As explained above, Zieminski voluntarily waived whatever right of privacy he might otherwise have had in the information he stored on the home computer. But even assuming that Zieminski has some lingering privacy interest in the information he stored on the home computer, we do not view TBG's demand for production as a serious invasion of that interest. (*Hill v. National Collegiate Athletic Assn., supra,* 7 Cal.4th at pp. 39–40, 26 Cal.Rptr.2d 834, 865 P.2d 633.) Appropriate protective orders can define the scope of TBG's inspection and copying of information on the computer to that which is directly relevant to

96 Cal.App.4th 443, 117 Cal.Rptr.2d 155, 18 IER Cases 545, 02 Cal. Daily Op. Serv. 1740, 2002 Daily Journal D.A.R 2091

this litigation, and can prohibit the unnecessary copying and dissemination of Zieminski's financial and other information that has no rational bearing on this case. (See *Britt v. Superior Court* (1978) 20 Cal.3d 844, 859, 143 Cal.Rptr. 695, 574 P.2d 766 [a party's waiver of his constitutional right to privacy must be narrowly rather than expansively construed, and compelled disclosure should be limited to information "essential to the fair resolution of the lawsuit"]; *Vinson v. Superior Court* (1987) 43 Cal.3d 833, 842, 239 Cal.Rptr. 292, 740 P.2d 404 [a plaintiff cannot be allowed to make serious allegations without affording the defendant an opportunity to put their truth to the test]; cf. *Harris v. Superior Court* (1992) 3 Cal.App.4th 661, 668, 4 Cal.Rptr.2d 564; *Save Open Space Santa Monica Mountains v. Superior Court* (2000) 84 Cal.App.4th 235, 255–256, 100 Cal.Rptr.2d 725.)

On remand, it will be up to Zieminski to identify with particularity the information ****165** that he claims ought to be excluded from TBG's inspection and copying; it will be up to the trial court to determine whether a protective order should issue and, if so, to determine the scope of the protection and the means by which production will be made (to insure compliance with the trial court's orders). (§ 2031, subd. (g).) We leave specifics to the parties and to the sound discretion of the trial court. (*Valley Bank of Nevada v. Superior Court* (1975) 15 Cal.3d 652, 658, 125 Cal.Rptr. 553, 542 P.2d 977.)

***455 DISPOSITION**

The petition is granted, and a writ will issue commanding the trial court (1) to vacate its order denying TBG's demand for production, (2) to enter a new order granting the motion and, following such further briefing and hearing as the court deems necessary and appropriate, (3) to decide the protective order issues. TBG is awarded its costs of these writ proceedings.

We concur: SPENCER, P.J., and ORTEGA, J.

Cal.App. 2 Dist.,2002.
TBG Ins. Services Corp. v. Superior Court
96 Cal.App.4th 443, 117 Cal.Rptr.2d 155, 18 IER Cases 545, 02 Cal. Daily Op. Serv. 1740, 2002 Daily Journal D.A.R. 2091

END OF DOCUMENT

2014 WL 7463887
Not Officially Published
(Cal. Rules of Court, Rules 8.1105 and 8.1110, 8.1115)
Only the Westlaw citation is currently available.

Court of Appeal,
Second District, Division 1, California.

AMERICAN INTERNATIONAL GROUP, INC., et al., Petitioners,
v.
The SUPERIOR COURT of Los Angeles County, Respondent;
Air Lease Corporation et al., Real Parties in Interest.

B258943 | Filed 12/23/2014

ORIGINAL PROCEEDING; petition for writ of mandate. Jane L. Johnson, Judge. Petition granted. (L.A.S.C. No. BC483370)

Attorneys and Law Firms

Morrison & Foerster, Arturo J. Gonzalez, Eric A. Tate and Tritia M. Murata for Petitioners American International Group, Inc., and International Lease Finance Corporation.

No appearance for Respondent.

Munger, Tolles & Olson, Mark B. Helm, Carolyn H. Luedtke, Laura D. Smolowe and Amelia L.B. Sargent for Real Party in Interest Air Lease Corporation.

Scheper Kim & Harris, Alexander H. Cote and Katherine Farkas for Real Party in Interest John Plueger.

OPINION AND ORDER GRANTING PEREMPTORY WRIT OF MANDATE

THE COURT:

***1** It is well established that where a company employee uses the company computer system to send and receive electronic communications (emails), those emails are not protected from disclosure to the company that owns the computer system, particularly when the employee acknowledged in writing that the employee had no right to privacy when using the computer system. The result is no different for a company executive.

In the case at bar, John Plueger, a former executive of American International Group, Inc., and International Lease Finance Corporation (collectively ILFC), executed an acknowledgement in writing that he had no right to privacy to the emails sent and received on ILFC computer system during his ILFC tenure. Because the emails were not private, they were not confidential and, thus, not subject to the protection of the attorney-client privilege.

Accordingly, we hold that ILFC is not obligated to "return, destroy, and otherwise make no use of emails" and reverse the challenged order.

BACKGROUND

ILFC sued Air Lease Corporation (ALC), Plueger, and others, for, inter alia, breach of fiduciary duty and misappropriation of trade secrets.[1] In the fifth amended complaint, ILFC alleges that Plueger was its chief operating officer (COO), but resigned and then became president and COO of a competing entity, defendant ALC.

ILFC has access to the emails that Plueger sent and received on ILFC computers during the period of time that he was in ILFC's employ. ALC and Plueger moved for an order compelling ILFC "to return, destroy, and otherwise make no use of any and all content of communications between Plueger and his attorneys that may be contained in any servers, computers, or other hard-copy or electronic media in their possession. [¶] This motion is made on the grounds that Plueger's communications with his counsel were privileged...."

Nearly two decades ago, on November 5, 1997, Plueger signed the Employee Acknowledgement, which provides in part: "I understand that my computer at ILFC and the software and files on my computer are ILFC property. I have no right to privacy with respect to any information on my computer or when using ILFC's E-mail or voicemail systems. ILFC and its Network Administrator have the right without my permission to delete any unauthorized software on my computer."

The Employee Acknowledgement begins: "This Personnel Policy Manual is an important document intended to help

you become acquainted with ILFC. This Manual will serve as a guide; it is not the final word in all cases. Individual circumstances may call for individual attention."

The manual provides in part:

"*Personal Use of ILFC E–Mail System and Internet Access*

"The e-mail system and internet access provided by ILFC are for conducting company business. ILFC recognizes that some personal business and communications occur today by e-mail or over the internet instead of telephone calls. Thus, as in the case with personal telephone calls, a certain level of personal e-mails will be sent and received at work. Similarly, some personal use of ILFC's internet services may be necessary or convenient. However, use of ILFC's e-mail and internet access services should be kept to a minimum and must not interfere with your work. To the extent possible, they should be made during the lunch hour, break periods or after hours.

***2** "[¶] ... [¶]

"*Monitoring of E–Mails and Internet Use for Non–Company Use and Pornographic or Inappropriate Content*

"An employee has no right to or expectation of privacy in his/her use of company computer systems or equipment. ILFC has the right to monitor, access, review, copy, delete, disclose and block an employee's e-mails, even those marked private, and monitor, disclose and block an employee's internet use without notice to or consent of the employee."

In his declaration in support of the motion, Plueger stated that he worked at ILFC for 24 years. In October 2008, Plueger and "other members of the ILFC management team" hired counsel, the law firm of Munger, Tolles & Olson LLP (MTO), for advice connected to the anticipated sale of ILFC by its parent. ILFC paid MTO "for all of the ILFC-related work MTO did on [Plueger's] behalf." From October 2008 through March 26, 2010, Plueger used ILFC equipment, as well as his personal computer, to communicate with MTO. Plueger quoted from the emails which contained an advising footer, stating that the email was confidential, protected by attorney-client privilege or the attorney work product doctrine and instructing the recipient to delete the email. Plueger further stated in his declaration that ILFC "fully authorized and endorsed" his use of MTO as counsel and paid MTO on his behalf.

Plueger stated that, as COO, he knew that ILFC did not monitor personal emails, except for two situations that did not apply to him: emails containing offensive language and emails from persons or companies forbidden to do business with U.S. companies. Based on his understanding of this practice, and the proviso in the Personnel Policy Manual that expressly states that the restriction on personal use of the ILFC computers is " 'a guide' " and " 'individual circumstances' " provided exceptions, Plueger believed that the emails sent to/from counsel were protected by the attorney-client privilege.

On the day he resigned, Plueger stated that an IT employee of ILFC created a hard drive of Plueger's personal files and gave the hard drive to Plueger. Plueger turned the hard drive over to his counsel, who identified 56 emails as protected by the attorney-client privilege.

On June 20, 2014, respondent court granted the motion. Respondent concluded that, while Plueger was bound by the policy, the policy, itself, "allows for exceptions based on circumstances." These circumstances include the employee manual's allowance of "a certain level of personal e-mails." Additionally, respondent court found that ILFC had hired and paid MTO to advise Plueger; the hiring and paying of the law firm constituted a basis for Plueger to have a reasonable belief that his "individual circumstances" exempted him from the general rule that e-mails between him and his counsel were not private.

The order was served electronically on the same day. ILFC did not seek appellate review of the order at that time. A formal order was filed on August 22. [2]

***3** ILFC filed its sixth amended complaint on September 11.

DISCUSSION

ILFC contends that Plueger's communications with MTO are not protected by the attorney-client privilege (Evid. Code, § 952), because Plueger had acknowledged in writing that he had no right to privacy in any communications made on ILFC equipment and that the trial court erred in concluding that "individual circumstances" gave Plueger license to ignore ILFC's clear technology-use policy. [3]

ALC and Plueger counter that substantial evidence supports the findings of respondent court that ILFC policy allowed for

individual circumstances where, in the case at bar, Plueger knew "for a fact" that ILFC was not reviewing the content of his emails, ILFC allowed for limited personal use of its computer equipment, and ILFC authorized and paid for Plueger's consultation with counsel. To the contrary, we are not bound by respondent court's interpretation of the employee handbook and Employee Acknowledgement, but review those written instruments de novo. (*Parsons v. Bristol Development Co.* (1965) 62 Cal.2d 861, 865; *Romo v. Y–3 Holdings, Inc.* (2001) 87 Cal.App.4th 1153, 1158.)

***4** It is the burden of ALC and Plueger, as the parties claiming privilege, to establish that the emails were sent in confidence. (*Costco Wholesale Corp. v. Superior Court* (2009) 47 Cal.4th 725, 733.) They did not carry this burden.

We agree with ILFC that Plueger had no reasonable expectation that the emails sent or received on ILFC equipment were confidential; accordingly, the subject electronic communications are not protected by the attorney-client privilege. [4] ILFC need not return, destroy, or otherwise refrain from using the emails.

Appellate review of discovery orders is appropriate where, as here, the order prevents a party from a fair litigation of the case. (*OXY Resources California LLC v. Superior Court* (2004) 115 Cal.App.4th 874, 886.)

In 2002, we held in *TBG Ins. Services Corp. v. Superior Court* (2002) 96 Cal.App.4th 443, 445, that the advance notice of employer TBG Insurance Services Corporation (TBG) to a senior executive, Robert Zieminski, combined with Zieminski's written consent to the policy, defeated the claim that Zieminski had a reasonable expectation of privacy in the TBG-provided computer he used at home. Zieminski, who had worked as a TBG senior executive for about 12 years, signed TBG's electronic and telephone equipment policy statement and agreed in writing that TBG had the right to monitor both of his computers. After TBG terminated Zieminski's employment for misuse of his office computer, Zieminski sued TBG for wrongful termination. The trial court denied TBG's motion to compel production of the home computer. TBG filed a petition for review in our Court. We concluded "that, given the employee's consent to his employer's monitoring of both computers, the employee had no reasonable expectation of privacy when he used the home computer for personal matters." (*Ibid.*)

Zieminski did not assert that the home computer contained privileged information. That question was addressed by the Third District in *Holmes v. Petrovich Development Co., LLC* (2011) 191 Cal.App.4th 1047 (*Holmes*). In *Holmes*, the Third District held that employee Gina Holmes's communications with her lawyer on her employer's computer equipment were not protected from disclosure by the attorney-client privilege. (*Id.* at p. 1051.) The Third District emphasized that the computer "belong[ed] to the [company]," that the company had a policy against using its computers for personal reasons, and that the employee was "aware of and agree[d] to these condition," going on to explain: "Holmes used her employer's company e-mail account after being warned that it was to be used only for company business, that e-mails were not private, and that the company would randomly and periodically monitor its technology resources to ensure compliance with the policy." (*Id.* at pp. 1068–1069.)

In *Holmes*, the Third District explained that the attorney-client privilege did not apply, because "Holmes used a computer of defendant company to send the e-mails even though (1) she had been told of the company's policy that its computers were to be used only for company business and that employees were prohibited from using them to send or receive personal e-mail, (2) she had been warned that the company would monitor its computers for compliance with this company policy and thus might 'inspect all files and messages ... at any time,' and (3) she had been explicitly advised that employees using company computers to create or maintain personal information or messages 'have no right of privacy with respect to that information or message.'.... [¶] [T]he e-mails sent via company computer under the circumstances of this case were akin to consulting her lawyer in her employer's conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard by him." (*Holmes, supra,* 191 Cal.App.4th at p. 1051.)

***5** Although ILFC did not regularly monitor electronic communications and may never have actually opened or reviewed any emails, ILFC had expressly warned in the Employee Acknowledgement that all files belong to ILFC and that there was "no right to privacy" in any information on the computer or in the emails. Plueger had signed the Employee Acknowledgement and does not deny that he knew what he was signing. ILFC's Personnel Policy Manual states that ILFC "has the right to monitor, access, review, copy,

delete, disclose and block an employee's e-mails, *even those marked private.*" (Italics added.)

That the emails sent between Plueger and MTO were marked as privileged does not override the express provisions that Plueger acknowledged in writing that he would have no privacy interest in them.

In issuing the order, respondent court cited language in the Personnel Policy Manual stating that it is a "guide" and "not the final word in all cases. Individual circumstances may call for individual attention." The manual recognizes that "a certain level of personal e-mails will be sent and received at work." The manual shows that ILFC intended a flexible application of the personnel policy, but it does not contradict the express statements that the computer system belongs to ILFC, which expressly warns its computer users that it can "monitor, access, review, copy, delete, disclose and block an employee's e-mails...." ILFC cautioned that "use of ILFC's e-mail and internet access services should be kept to a minimum," and certainly did not give Plueger carte blanche to use ILFC's computer system.

It was not reasonable for Plueger to believe that his communications with counsel on ILFC computers were private; thus, by using the computer system that ILFC was free to monitor, Plueger's communications were not private nor confidential.

That ILFC hired and paid for MTO to represent Plueger individually in 2008–2010 does not support his claim of confidentiality. Plueger asserts that ILFC's hiring and paying the law firm constituted approval of Plueger's communications with the firm and its permission to use ILFC's computer, thus ILFC implicitly acknowledged that the attorney-client privilege protected the communications. To the contrary, given that Plueger stated in his declaration that in October 2008, Plueger and "other members of the ILFC management team" hired MTO and that MTO *continues* to represent ILFC, Plueger was aware that MTO served two masters. At the time he communicated with the firm, Plueger—as COO and as part of the management team that hired MTO to represent ILFC—knew that MTO was ILFC's law firm and, thus, Plueger was aware that the firm had dual loyalties to both Plueger and ILFC. Any expectation of confidentiality of communications between the firm and Plueger would have been unreasonable.

For the aforementioned reasons, Plueger's email communications via the ILFC computer system are not confidential and, thus, are not protected from disclosure by the attorney-client privilege.

Accordingly, as there is not a plain, speedy and adequate remedy at law, and in view of the fact that the issuance of an alternative writ would add nothing to the presentation already made, we deem this to be a proper case for the issuance of a peremptory writ of mandate "in the first instance." (Code Civ. Proc., § 1088; *Brown, Winfield & Canzoneri, Inc. v. Superior Court* (2010) 47 Cal.4th 1233, 1237–1238; *Lewis v. Superior Court* (1999) 19 Cal.4th 1232, 1240–1241.) Opposition was requested and the parties were notified of the court's intention to issue a peremptory writ. (*Palma v. U.S. Industrial Fasteners, Inc.* (1984) 36 Cal.3d 171, 180.)

DISPOSITION

***6** THEREFORE, let a peremptory writ issue, commanding respondent superior court to vacate its August 22, 2014 order, granting the motion for return, destruction and nonuse of John Plueger's email communications stored on International Lease Finance Corporation's computer hard drives, and to issue a new and different order denying same, in Los Angeles Superior Court case No. BC483370, entitled American International Group, Inc., et al. v. Air Lease Corporation et al.

All parties shall bear their own costs.

.

ROTHSCHILD, P.J.

CHANEY, J.

JOHNSON, J.

Footnotes

1 Both are in the business of airplane leases and come under limited federal scrutiny.

2 We reject the contention of ALC and Plueger that we should forgo the granting of relief because of the timing of the filing of the writ petition. We note that ALC and Plueger acknowledge that respondent court filed a formal order on August 22, 2014. The petition, filed September 19, 2014, was filed just under one month after the filing of the formal order.

3 Evidence Code section 952 provides: "As used in this article, 'confidential communication between client and lawyer' means information transmitted between a client and his or her lawyer in the course of that relationship and in confidence by a means which, so far as the client is aware, discloses the information to no third persons other than those who are present to further the interest of the client in the consultation or those to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted, and includes a legal opinion formed and the advice given by the lawyer in the course of that relationship."

Evidence Code section 954 provides in relevant part: "Subject to Section 912 and except as otherwise provided in this article, the client, whether or not a party, has a privilege to refuse to disclose, and to prevent another from disclosing, a confidential communication between client and lawyer...."

Evidence Code section 917 states in relevant part: "(a) If a privilege is claimed on the ground that the matter sought to be disclosed is a communication made in confidence in the course of the lawyer-client ... relationship, the communication is presumed to have been made in confidence and the opponent of the claim of privilege has the burden of proof to establish that the communication was not confidential. [¶] (b) A communication ... does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication...."

Evidence Code section 912, subdivision (a) provides that the holder of the privilege waives the privilege where the "holder of the privilege, without coercion, has disclosed a significant part of the communication or has consented to disclosure made by anyone. Consent to disclosure is manifested by any statement or other conduct of the holder of the privilege indicating consent to the disclosure, including failure to claim the privilege in any proceeding in which the holder has the legal standing and opportunity to claim the privilege."

4 In *Doe v. City & County of San Francisco* (N.D. Cal. 2011) 835 F. Supp.2d 762, 769, the district court held that there was no violation of Federal Stored Communications Act (18 U.S.C. § 2702) in review of employee emails.

End of Document

--- F.Supp.2d ----, 2014 WL 4274313 (N.D.Cal.), 2014 IER Cases 167,127
(Cite as: 2014 WL 4274313 (N.D.Cal.))

H

United States District Court,
Oakland Division.
Oakland Division
Sunbelt Rentals, Inc., Plaintiff,
v.
Santiago Victor, Defendant.

Case No: C 13–4240 SBA
4:13–cv–04240Signed August 28, 2014

Background: Employer filed suit against terminated sales representative alleging breach of contract, misappropriation of trade secrets, unfair competition and breach of duty of loyalty. Employee counterclaimed alleging violation of his right to privacy, and violations of federal Wiretap Act, Stored Communications Act (SCA), and California Penal Code, based on employer's review of text messages contained on his employer-issued cellular telephone and content contained on his employer-issued electronic device. Plaintiff moved to dismiss defendant's counterclaims.

Holdings: The District Court, Saundra Brown Armstrong, J., held that:
(1) complaint failed to state claim for violation of Wiretap Act;
(2) complaint failed to state claim for violation of California's law governing unauthorized access to computers; and
(3) complaint failed to state claim for a privacy violation based on California's common law tort of intrusion.

Motion granted.

West Headnotes

[1] Telecommunications 372 1436

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General
372k1435 Acts Constituting Interception or Disclosure
372k1436 k. In general. Most Cited Cases

Under federal Wiretap Act, “acquisition” of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device occurs when the contents of a wire communication are captured or redirected in any way. 18 U.S.C.A. § 2511(1)(a).

[2] Telecommunications 372 1447

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General
372k1442 Actions
372k1447 k. Pleading. Most Cited Cases

Employee's complaint against former employer failed to sufficiently allege that his employer had “intentionally” intercepted text messages sent from his employer-issued cellular telephone, as required to state claim for violation of federal Wiretap Act; complaint alleged only that after his termination, when former employee “synced” his old telephone account to his new employer's telephone, that text messages had “appeared” on the old phone issued to him by his former employer. 18 U.S.C.A. § 2511(1)(a).

[3] Telecommunications 372 1436

--- F.Supp.2d ----, 2014 WL 4274313 (N.D.Cal.), 2014 IER Cases 167,127
(Cite as: 2014 WL 4274313 (N.D.Cal.))

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General
372k1435 Acts Constituting Interception or Disclosure
372k1436 k. In general. Most Cited Cases

For a communication to be "intercepted" under federal Wiretap Act, it must be acquired during transmission, not while it is in electronic storage. 18 U.S.C.A. § 2511(1)(a).

[4] Telecommunications 372 1438

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General
372k1435 Acts Constituting Interception or Disclosure
372k1438 k. Wireless or mobile communications. Most Cited Cases

Employee's allegations that his former employer read his text messages after they were sent and received on the his employer-issued cellular telephone were insufficient to demonstrate intentional "interception," as would violate federal Wiretap Act. 18 U.S.C.A. § 2511(1)(a).

[5] Telecommunications 372 1438

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General
372k1435 Acts Constituting Interception or Disclosure
372k1438 k. Wireless or mobile communications. Most Cited Cases

Unless some type of automatic routing software is used to divert a text message, interception of a text message within the prohibition of the Wiretap Act is virtually impossible. 18 U.S.C.A. § 2511(1)(a).

[6] Telecommunications 372 1438

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General
372k1435 Acts Constituting Interception or Disclosure
372k1438 k. Wireless or mobile communications. Most Cited Cases

Text messages and pictures stored on a cellular telephone do not constitute "electronic storage" for purposes of Stored Communications Act (SCA); rather, electronic storage is either temporary, intermediate storage incidental to electronic transmission, or storage for purposes of backup protection. 18 U.S.C.A. §§ 2701(a)(1), 2707(a); 28 U.S.C.A. § 2510(17).

[7] Telecommunications 372 1342

372 Telecommunications
372VIII Computer Communications
372k1339 Civil Liabilities; Illegal or Improper Purposes
372k1342 k. Fraud; unauthorized access or transmission. Most Cited Cases

California law prohibiting unauthorized access to computers, computer systems, and computer networks is an anti-hacking statute intended to prohibit the unauthorized use of any computer system for improper or illegitimate purposes. Cal. Penal Code § 502.

--- F.Supp.2d ----, 2014 WL 4274313 (N.D.Cal.), 2014 IER Cases 167,127
(Cite as: 2014 WL 4274313 (N.D.Cal.))

[8] Telecommunications 372 1342

372 Telecommunications
372VIII Computer Communications
372k1339 Civil Liabilities; Illegal or Improper Purposes
372k1342 k. Fraud; unauthorized access or transmission. Most Cited Cases

A party acts "without permission" within meaning of California law governing unauthorized access to computers, computer systems, and computer data, when they circumvent technical or code-based barriers in place to restrict or bar a user's access. Cal. Penal Code § 502.

[9] Telecommunications 372 1342

372 Telecommunications
372VIII Computer Communications
372k1339 Civil Liabilities; Illegal or Improper Purposes
372k1342 k. Fraud; unauthorized access or transmission. Most Cited Cases

Even if employer accessed terminated employee's private electronic data and electronic communications through his cellular telephone provider's computer network, such access did not violate California law governing unauthorized access to computers, computer systems, and computer data, absent proof that employer had done so by circumventing technical or code-based barriers intended to restrict such access. Cal. Penal Code § 502.

[10] Torts 379 329

379 Torts
379IV Privacy and Publicity
379IV(A) In General
379k329 k. Types of invasions or wrongs recognized. Most Cited Cases

California law recognizes four categories of the tort of invasion of privacy: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light in the public eye; and (4) appropriation of name or likeness.

[11] Torts 379 340

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)2 Intrusion
379k340 k. In general. Most Cited Cases

Under California law, a privacy violation based on the common law tort of intrusion has two elements: (1) defendant must intentionally intrude into a place, conversation, or matter as to which plaintiff has a reasonable expectation of privacy, and (2) the intrusion must occur in a manner highly offensive to a reasonable person.

[12] Torts 379 340

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)2 Intrusion
379k340 k. In general. Most Cited Cases

Under California law, a privacy violation based on the common law tort of intrusion is proven only if plaintiff had an objectively reasonable expectation of seclusion or solitude in the place, conversation, or data source.

[13] Torts 379 344

379 Torts
379IV Privacy and Publicity

--- F.Supp.2d ----, 2014 WL 4274313 (N.D.Cal.), 2014 IER Cases 167,127
(Cite as: 2014 WL 4274313 (N.D.Cal.))

379IV(B) Privacy
379IV(B)2 Intrusion
379k344 k. Waiver or consent. Most Cited Cases

Under California law, a plaintiff pursuing an invasion of privacy action must have conducted himself or herself in a manner consistent with an actual expectation of privacy, i.e., he or she must not have engaged in conduct which manifests a voluntary consent to the invasive actions of defendant.

[14] Torts 379 341

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)2 Intrusion
379k341 k. Particular cases in general. Most Cited Cases

Torts 379 415

379 Torts
379IV Privacy and Publicity
379IV(D) Actions in General
379k415 k. Pleading. Most Cited Cases

Under California law, employee's vague allegations that his former employer acted in a "highly offensive manner" by "accessing, intercepting, monitoring, reviewing, storing, and using" his post-employment private electronic data and electronic communications displayed on an employer-issued cellular telephone, after it had been returned to the company upon employee's departure, failed to state a claim for a privacy violation based on the common law tort of intrusion; former employee had no legally protected privacy interest or reasonable expectation of privacy in electronic messages, in general, and it was unclear whether he was asserting a privacy interest with respect to the contents of those communications, to which a privacy interest could attach.

[15] Torts 379 341

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)2 Intrusion
379k341 k. Particular cases in general. Most Cited Cases

Under California law, terminated employee failed to conduct himself in a manner consistent with an actual expectation of privacy in text messages on his cellular telephone, and thus lacked the objectively reasonable expectation of privacy required to establish invasion of privacy by former employer that viewed messages on a cellular telephone previously issued to employee and returned upon his termination, since when former employee "synced" his new devices he failed to first unlink his prior employer-issued telephone from his account, thus personally causing the transmissions to it.

Joseph C. Wilson, Michelle Therese Duval, Richard James Curiale, Curiale Wilson LLP, Allison Marie Dibley, Esq., Joseph C. Wilson, V, Nossaman LLP, San Francisco, CA, Patricia Jeanne Hill, Yash B. Dave, Smith, Gambrell & Russell, LLP, Jacksonville, FL, Veronica Meryl Gray, Nossaman LLP, Irvine, CA, for Plaintiff.

Beth Ann Kahn, Kevin M. Pollack, Kurt Alan Dreibholz, Morris Polich Purdy, Los Angeles, CA, for Defendant.

ORDER GRANTING PLAINTIFF'S MOTION TO DISMISS DEFENDANT'S COUNTER-CLAIMS

Dkt. 39

SAUNDRA BROWN ARMSTRONG, United States

--- F.Supp.2d ----, 2014 WL 4274313 (N.D.Cal.), 2014 IER Cases 167,127
(Cite as: 2014 WL 4274313 (N.D.Cal.))

District Judge

***1 Sunbelt Rentals**, Inc. ("Plaintiff" or "Sunbelt") filed the instant action against its former employee, Santiago Victor ("Defendant" or "Victor"), alleging that he misappropriated trade secrets upon his termination. Victor has filed five counterclaims against Sunbelt, accusing it, inter alia, of violating the federal Wiretap Act and the Stored Communications Act ("SCA") by reviewing his text messages on the iPhone which Sunbelt had previously issued to him. The parties are presently before the Court on Plaintiff's Motion to Dismiss Defendants Counterclaims. Having read and considered the papers filed in connection with this matter and being fully informed, the Court hereby GRANTS the motion and dismisses Victor's counterclaims, with leave to amend. The Court, in its discretion, finds this matter suitable for resolution without oral argument. Fed.R.Civ.P. 78(b); N.D. Cal. Civ. L.R. 7–1(b).

I. *BACKGROUND*

A. RELEVANT FACTS

During the relevant time period, Victor worked as an outside sales representative for Sunbelt, an equipment rental company. Countercl. ¶ 11, Dkt. 34. In August 2013, Victor gave his two-week notice to Sunbelt, stating that he had taken a job with one of its competitors—Ahern Rentals ("Ahern"). *Id.* ¶ 16. Upon learning of Victor's intent to leave the company, Sunbelt immediately dismissed him. *Id.*

During his time with Sunbelt, Victor was assigned a Sunbelt-owned iPhone ("Sunbelt iPhone") and a Sunbelt-owned iPad for both **work** and **personal** purposes. *Id.* ¶¶ 12–14. Thereafter, Victor "created and paid for a **personal** 'Apple account' that was linked to both devices." *Id.* ¶ 15. Victor returned the devices to Sunbelt after his separation. *Id.* ¶¶ 16, 18, 20.

Victor's new employer, Ahern, provided him a new iPhone ("Ahern iPhone"). *Id.* ¶ 19–20. At some point thereafter, Victor registered or linked his Ahern iPhone to the same **personal** Apple account he had previously used while at Sunbelt. *Id.* ¶ 19. This process "synced" Victor's Ahern iPhone with his **personal** Apple account. *Id.*

Several weeks later, when he received a new iPad from Ahern ("Ahern iPad"), Victor linked the new iPad to his **personal** Apple account. *Id.* ¶ 20. In the process of registering the Ahern iPad, Victor discovered the telephone number associated with the Sunbelt iPhone was still linked to his **personal** Apple account. *Id.* Because Victor had failed to unlink the Sunbelt iPhone from his account, his "private electronic data and electronic messages," including text messages sent to and from his Ahern iPhone, also were transmitted to the Sunbelt iPhone which he had returned to Sunbelt. *Id.* ¶ 20, 21. Victor then deleted the Sunbelt number from his account "to ensure that his new Ahern issued Apple products were not in any way linked to Sunbelt." *Id.*

Victor claims that after his departure, Sunbelt "began actively investigating Victor's post-employment acts, conduct, and communications." *Id.* ¶ 21. In the course of such investigation, Sunbelt allegedly "invaded Victor's privacy rights by ***accessing, intercepting, monitoring, reviewing, storing and using*** Victor's post-employment private electronic data and electronic communications (including but not limited to ***text messages*** sent and received from Victor's Ahern, Rentals Inc. issued iPhone) without authority, permission, or consent." *Id.* (emphasis added). Victor further accuses Sunbelt of "***intentionally accessing*** Victor's private electronic communications and data, without authorization, from facilities through which Victor's electronic communications were provided and stored (i.e., Victor's cellular phone provider's network which stores Victor's electronic communications, and or Apple's cloud based network where Victor's electronic communica-

tion pertaining to his Apple Account are processed and stored) and where such services and communications were restricted to access by Victor, which Sunbelt obtained through improper means." *Id.* ¶ 23 (emphasis added). No particular facts are alleged to support these assertions.

B. PROCEDURAL HISTORY

***2** On September 12, 2013, Sunbelt filed a complaint against Victor in this Court alleging four state law causes of action: (1) breach of contract; (2) misappropriation of trade secrets; (3) unfair competition; and (4) breach of duty of loyalty. Dkt. 1. Victor then filed an Answer, and later amended an Answer and Counterclaim. The gist of the Counterclaim is that Sunbelt improperly read the text messages that were inadvertently transmitted to his Sunbelt iPhone. He alleges claims for violations of: (1) the Wiretap Act; (2) the SCA; (3) California Penal Code § 502 et seq; (4) California Penal Code § 630 et seq; and (5) his right to privacy. *See* Countercl. ¶ 24. Each of these claims is based on the same set of facts—Sunbelt's purported interception, acquisition and use of Victor's electronic communications (i.e., text messages) sent to and from his Ahern iPhone. Sunbelt now moves to dismiss all counterclaims. This matter has been fully briefed and is ripe for adjudication.

II. *LEGAL STANDARD*

Pleadings in federal court actions are governed by Federal Rule of Civil Procedure 8(a)(2), which requires only "a short and plain statement of the claim showing that the pleader is entitled to relief." Rule 12(b)(6) "tests the legal sufficiency of a claim." *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir.2001). A complaint may be dismissed under Rule 12(b)(6) for either failure to state a cognizable legal theory or insufficient facts to support a cognizable legal theory. *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir.2008). "[C]ourts must consider the complaint in its entirety, as well as other sources courts ordinarily examine when ruling on Rule 12(b)(6) motions to dismiss, in particular, documents incorporated into the complaint by reference, and matters of which a court may take judicial notice." *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322, 127 S.Ct. 2499, 168 L.Ed.2d 179 (2007) The court is to "accept all factual allegations in the complaint as true and construe the pleadings in the light most favorable to the nonmoving party." *Outdoor Media Group, Inc. v. City of Beaumont*, 506 F.3d 895, 899–900 (9th Cir.2007).

To survive a motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.' " *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007)). The complaint must afford the defendants with "fair notice" of the claims against them, and the grounds upon which the claims are based. *Swierkiewicz v. Sorema N.A.*, 534 U.S. 506, 512, 122 S.Ct. 992, 152 L.Ed.2d 1 (2002). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Iqbal*, 556 U.S. at 678, 129 S.Ct. 1937. When a complaint or claim is dismissed, "[l]eave to amend should be granted unless the district court determines that the pleading could not possibly be cured by the allegation of other facts." *Knappenberger v. City of Phoenix*, 566 F.3d 936, 942 (9th Cir.2009).

III. *DISCUSSION*

A. WIRETAP ACT

[1]The Wiretap Act imposes civil liability against any person who "***intentionally intercepts,*** endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C §§ 2511(1)(a) (emphasis added); *id.* § 2520(a). The Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the

use of any electronic, mechanical, or other device."18 U.S.C. § 2510(4). "Such acquisition occurs 'when the contents of a wire communication are captured or redirected in any way.' " *Noel v. Hall*, 568 F.3d 743, 749 (9th Cir.2009). The inception must be intentional, as opposed to inadvertent. *See Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 742–43 (4th Cir.1994).

[2]Here, Victor has failed to allege facts sufficient to establish that Sunbelt "intentionally intercepted" any of his text messages. By Victor's own account, the text messages appeared on his Sunbelt iPhone as a result of Victor's act of syncing his new iPhone to his Apple account without first un-linking his Sunbelt iPhone. Countercl. ¶¶ 19, 20. In other words, Sunbelt did not intentionally capture or redirect Victor's text messages to the Sunbelt iPhone—the transmission of those messages was entirely Victor's doing. Given these circumstances, the requisite intentional conduct is lacking. *Sanders*, 38 F.3d at 742–43; *Shubert v. Metrophone, Inc.*, 898 F.2d 401, 405 (3rd Cir.1990) (noting that Congress specifically intended that "inadvertent interceptions are not crimes under [the Wiretap Act]").

3** [3][4]Nor has Victor alleged facts sufficient to establish that Sunbelt acted to "intercept" the text messages or any other electronic communications. The Ninth Circuit applies a "narrow definition of 'intercept.' " *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir.2002). For a communication to be intercepted, "it must be acquired during transmission, not while it is in electronic storage." *Id.* Though Victor vaguely alleges that Sunbelt intercepted his electronic communications, i.e., his text messages, he provides no facts to support this otherwise conclusory assertion.[FN1] If anything, the pleadings suggest that Sunbelt read Victor's text messages ***after they were sent and received on the Sunbelt iPhone, which is insufficient to demonstrate intentional interception under the Wiretap Act. *See NovelPoster v. Javitch Canfield Group*, No. C 13–5186 WHO, 2014 WL 3845148, *10 (N.D.Cal. Aug. 14, 2014) (reading emails that have already been received in an email account's inbox does not constitute interception under the Wiretap Act because the transmission had already occurred).

FN1. Victor's Counterclaim repeatedly makes vague and formulaic references to "private and electronic communications," but only specifically identifies "text messages" as having been allegedly intercepted. *See* Countercl. ¶ 22. Victor never specifies how the alleged interception transpired.

[5]Although it is clear that Victor's Wiretap Act claim must be dismissed, what is less clear is whether leave to amend should be granted. Given the almost instantaneous transmission of text messages, the window during which an interception may occur is exceedingly narrow. *NovelPoster*, 2014 WL 3845148, *10 (citing *United States v. Steiger*, 318 F.3d 1039, 1050 (11th Cir.2003)). Thus, "unless some type of automatic routing software is used" to divert the text message, interception of [a text message] within the prohibition of the Wiretap Act is virtually impossible." *Id.* (internal quotations and citation omitted). Given these constraints, it is doubtful that Victor will be able to allege facts, consistent with Federal Rule of Civil Procedure 11, to state a claim for violation of the Wiretap Act. Nonetheless, the Court will afford Victor an opportunity to amend this claim and therefore DISMISSES his claim under the Wiretap Act, with leave to amend.[FN2]

FN2. Sunbelt also contends that Victor has failed to allege any facts showing that it intercepted his text messages "through the use of any ... device." 18 U.S.C. § 2510(4) (emphasis added). Since it is clear that the Counterclaim fails to allege intentional interception, the Court need not reach that issue at this juncture.

B. STORED COMMUNICATIONS ACT

The SCA creates "a cause of action against anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided ... and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage.' " *Theofel v. Farey–Jones*, 359 F.3d 1066, 1072 (9th Cir.2004) (quoting 18 U.S.C. §§ 2701(a)(1), 2707(a)). "[E]lectronic storage" is defined as either "temporary, intermediate storage ... incidental to ... electronic transmission," or "storage ... for purposes of backup protection." 28 U.S.C. § 2510(17).

[6]According to Victor, Sunbelt violated the SCA by virtue of having,

> Intentionally accessed, without authorization, facilities through which Victor's electronic communications were provided and stored (i.e., Victor's cellular phone provider's network which stores Victor's electronic communications, and or Apple's cloud based network where Victor's electronic communication pertaining to his Apple Account are processed and stored) and where such services and communications were restricted to access by Victor, which Sunbelt obtained through improper means.

Countercl. ¶ 45. No facts are presented, however, to support the conclusory assertion that Sunbelt ***accessed*** Victor's text messages through his cellular telephone provider or Apple's network. Moreover, in his opposition, Victor contradicts himself by stating that the text messages allegedly accessed by Sunbelt "were ***not*** accessed through, nor stored on a website." Opp'n at 4 (emphasis added). To the extent that Victor is claiming that Sunbelt accessed his text messages by reviewing the messages on his Sunbelt iPhone—as he does elsewhere in his Counterclaim, such conduct does not violate the SCA. *See Garcia v. City of Laredo, Tex.*, 702 F.3d 788, 793 (5th Cir.2012) (holding that text messages and pictures stored on a cellular telephone do not constitute "electronic storage" for purposes of the SCA). This claim is DISMISSED with leave to amend.

C. CALIFORNIA PENAL CODE § 502

***4** [7]Section 502 of the California Penal Code prohibits unauthorized access to computers, computer systems, and computer networks, and provides for a civil remedy in the form of compensatory damages, injunctive relief, and other equitable relief. Cal.Penal Code § 502. Section 502 is an anti-hacking statute intended to prohibit the unauthorized use of any computer system for improper or illegitimate purpose. *Yee v. Lin*, No. C 12–02474 WHA, 2012 WL 4343778, *2 (N.D.Cal. Sept. 20, 2012).

[8]Victor alleges that Sunbelt violated subsections (c)(1), (2), (3), (4), (6), and (7) of Section 502, which provides that a person is liable if he:

> (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.
>
> (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
>
> (3) Knowingly and without permission uses or causes to be used computer services.
>
> (4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs

> which reside or exist internal or external to a computer, computer system, or computer network.
>
> ...
>
> (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
>
> (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network."

Id. § 502(c); Countercl. ¶ 54. For purposes of Section 502, parties act "without permission" when they "circumvent[ ] technical or code-based barriers in place to restrict or bar a user's access." *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.Supp.2d 1025, 1036 (N.D.Cal.2012).

[9]In his third Counterclaim, Victor alleges as follows:

> On information and belief, Sunbelt violated California Penal Code section 502 when it improperly began accessing, intercepting, monitoring, reviewing and using Victor's post-employment private electronic data and electronic communications without Victor's knowledge, authorization or consent. On information and belief, Sunbelt additionally, or in the alternative, violated of Penal Code § 502 ***by intentionally accessing, without authorization,*** facilities through which Victor's electronic communications were provided and stored (i.e., Victor's cellular phone provider's network which stores Victor's electronic communications, and or Apple's cloud based network where Victor's electronic communication pertaining to his Apple Account are processed and stored) and where such services and communications were restricted to access by Victor, which Sunbelt obtained through improper means.

Countercl. ¶ 56 (emphasis added). These fact-barren and vague allegations are precisely the type of "threadbare recitals" proscribed by *Twombly* and *Iqbal*. Moreover, to the extent that Victor is claiming that Sunbelt accessed his unspecified "private electronic data and electronic communications" through the Apple account or his cellular telephone provider's computer network, such a claim fails on the ground that no facts are alleged showing that Sunbelt did so by circumventing technical or code-based barriers intended to restrict such access. *Facebook*, 844 F.Supp.2d at 1036. To the contrary, Victor simply avers that Sunbelt reviewed his text messages that he caused, albeit inadvertently, to be sent to the Sunbelt iPhone. The Court therefore concludes that Victor has failed to state a claim under Section 502 and DISMISSES said claim with leave to amend.

D. CALIFORNIA PENAL CODE § 630

***5** The California Invasion of Privacy Act ("CIPA") is intended to prevent privacy invasions facilitated by modern technology and devices. Cal.Penal Code § 630. "The analysis for a violation of CIPA is the same as that under the federal Wiretap Act." *NovelPoster*, 2014 WL 3845148, *12 (granting judgment on pleadings on CIPA claim for same reasons underlying the dismissal of the plaintiff's Wiretap Act claim, i.e., the lack of intentional interception). As discussed, Victor has failed to plausibly allege a violation of the Wiretap Act; *a fortiori*, he is also unable to allege a violation of CIPA. This claim is DISMISSED with leave to amend.

E. INVASION OF PRIVACY

[10]California recognizes four categories of the tort of invasion of privacy: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light in the public eye; and (4) appropriation of name or likeness. *Shulman v. Group W Prods., Inc.*, 18

Cal.4th 200, 214 n. 4, 74 Cal.Rptr.2d 843, 955 P.2d 469 (1998). Victor fails to indicate which type of invasion of privacy claim he is alleging. Nonetheless, based on the sparse allegations presented, it appears that he is attempting to state a claim for intrusion upon seclusion.

[11][12][13]"A privacy violation based on the common law tort of intrusion has two elements. First, the defendant must intentionally intrude into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy. Second, the intrusion must occur in a manner highly offensive to a reasonable person." *Hernandez v. Hillsides, Inc.*, 47 Cal.4th 272, 285, 97 Cal.Rptr.3d 274, 211 P.3d 1063 (2009). "The tort is proven only if the plaintiff had an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source." *Shulman v. Grp. W Prods., Inc.*, 18 Cal.4th 200, 232, 74 Cal.Rptr.2d 843, 955 P.2d 469 (1998). A plaintiff pursuing an invasion of privacy action must have conducted himself or herself in a manner consistent with an actual expectation of privacy, i.e., he or she must not have engaged in conduct which manifests a voluntary consent to the invasive actions of defendant. *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal.4th 1, 26, 26 Cal.Rptr.2d 834, 865 P.2d 633 (1994).

[14]Victor contends that, as a matter of law, an employee has a reasonable expectation of privacy with respect to text messages contained on employer-owned mobile telephones. The decisional authorities cited by Victor, however, are inapposite. In *City of Ontario v. Quon*, 560 U.S. 746, 130 S.Ct. 2619, 177 L.Ed.2d 216 (2010), a police officer was issued a pager by his police department which was subject to a limit on the number of characters that could be sent and received each month. *Id.* at 750, 130 S.Ct. 2619. After becoming concerned that the officer was repeatedly exceeding his character limit, the police department obtained transcripts of the text messages from the wireless carrier to ascertain whether the texts were **work**-related or **personal**. *Id.* at 750–51, 130 S.Ct. 2619. After finding that most of the text messages were not **work**-related, the police department took disciplinary action against the officer. *Id.* at 753, 130 S.Ct. 2619. The police officer then brought an action under 42 U.S.C. § 1983 against the city, police department and police chief, alleging that the police department's review of his text messages violated the Fourth Amendment.

In the addressing the plaintiff's Fourth Amendment claim, the United States Supreme Court ***assumed, without deciding,*** that the plaintiff had a reasonable expectation of privacy in text messages sent to him on an employer-provided pager; however, the Court ultimately upheld the police department's review of those messages as reasonable under the Fourth Amendment. *Id.* at 760, 130 S.Ct. 2619. Despite Victor's suggestion to the contrary, the Supreme Court did not hold that an employee automatically has an expectation of privacy in electronic messages stored on a device provided by his employer. *Quon* also is distinguishable on its facts. Unlike the police officer in *Quon*, Victor was no longer an employee of the company that owned the electronic device at issue at the time the invasion of privacy allegedly occurred. Moreover, unlike the police department, which requested transcripts of the text messages from the wireless carrier, Sunbelt is not alleged to have affirmatively undertaken any action to obtain and review the text messages or any other electronic data. Rather, the electronic communications appeared on Sunbelt's iPhone because of actions taken by Victor.

***6** Victor's citation to *United States v. Finley*, 477 F.3d 250 (5th Cir.2007) fares no better. In that case, a criminal defendant challenged the denial of his motion to suppress text messages and call records which law enforcement officials had obtained through a warrantless search of his employer-issued cell phone. In addressing the threshold issue of whether the defendant had standing to raise a Fourth Amendment challenge, the Fifth Circuit held that the mere fact that the employer owned the phone and had access to its con-

tents did not ipso facto demonstrate that defendant correspondingly had no expectation of privacy in his call records and text messages. *Id.* at 259. In reaching its decision, the court specifically noted that the defendant had undertaken precautions to maintain the privacy of data stored on his phone and that he "had a right to exclude others from using the phone." *Id.* Unlike the defendant in *Finley,* Victor was no longer an employee of the company which owned the cell phone to which the subject text messages had been sent. In addition, Victor had no right to exclude others from accessing the Sunbelt iPhone—which he did not own or possess and no longer had any right to access. Moreover, rather than undertake precautions to maintain the privacy of his text messages, Victor did just the opposite by failing to unlink his Sunbelt iPhone from his Apple account, which, in turn, facilitated the transmission of those messages to an iPhone exclusively owned, controlled and possessed by his former employer.

[15]Victor's privacy claim also fails on the ground that he has failed to show an intrusion into a "place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy." *Hernandez,* 47 Cal.4th at 285, 97 Cal.Rptr.3d 274, 211 P.3d 1063. As noted, Victor cannot legitimately claim an expectation of privacy in a "place," i.e., the Sunbelt iPhone, which belongs to his former employer and to which he has no right to access. Nor can Victor claim a reasonable expectation of privacy with respect to his text messages, in general. The pleadings do not identify the contents of any particular text messages, and instead, refer generally to "private electronic data and electronic communications." Countercl. ¶ 79. This and other courts have concluded that there is no "legally protected privacy interest and reasonable expectation of privacy" in electronic messages, "in general."*In re Yahoo Mail Litig.,* —— F.Supp.2d ——, ——,2014 WL 3962824, *16 (N.D.Cal. Aug. 12, 2014) (citing cases).[FN3] Rather, a privacy interest can exist, if at all, only with respect to the ***content*** of those communications. In any event, even if Victor were claiming an expectation of privacy with respect to the specific content of his text messages (which he has not specified), the facts alleged demonstrate that he failed to comport himself in a manner consistent with an objectively reasonable expectation of privacy. By his own admission, Victor personally caused the transmission of his text messages to the ***Sunbelt*** iPhone by syncing his new devices to his Apple account without first unlinking his Sunbelt iPhone.[FN4] As such, even if he ***subjectively*** harbored an expectation of privacy in his text messages, such expectation cannot be characterized as ***objectively*** reasonable, since it was ***Victor's*** conduct that directly caused the transmission of his text messages to Sunbelt in the first instance. *See Hill,* 7 Cal.4th at 26, 26 Cal.Rptr.2d 834, 865 P.2d 633.

FN3. Victor also does not specify whether his claim is predicated upon text messages sent by him, received by him, or both. With respect to messages he transmitted, there is authority finding that a plaintiff has no reasonable expectation of privacy in messages sent to third parties. *See Fetsch v. City of Roseburg,* No. 6:11–cv–6343–TC, 2012 WL 6742665, *10 (D.Or. Dec. 31, 2012) (plaintiff had no expectation of privacy in text messages sent from his phone because relinquished control of them once they were transmitted).

FN4. Victor vaguely alleges that Sunbelt intercepted his electronic communications. He provides no factual support for this conclusory assertion. *See* Countercl. ¶ 77.

The above notwithstanding, the facts alleged in Victor's fifth counterclaim are insufficient to show that Sunbelt intruded into Victor's privacy in a manner highly offensive to a reasonable person. "Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms

underlying the privacy right." *Hill*, 7 Cal.4th at 37, 26 Cal.Rptr.2d 834, 865 P.2d 633. In addition, the plaintiff must show "that the ***use*** of plaintiff's information was highly offensive." *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal.App.4th 986, 993, 125 Cal.Rptr.3d 260 (2011) (emphasis added) (upholding the demurrer to plaintiff's common law invasion of privacy claim where, finding that even if the customer addresses were obtained through "questionable" means, there was "no allegation that Lamps Plus used the address once obtained for an offensive or improper purpose.").

***7** Here, Victor alleges only that Sunbelt acted in a "highly offensive" manner by "accessing, intercepting, monitoring, reviewing, storing and using [his] post-employment private electronic data and electronic communications without [his] knowledge, authorization or consent as part of an unreasonably intrusive and unauthorized investigation into Victor's post-employment conduct." Countercl. ¶ 79. Victor offers no factual support for these conclusory assertions. In particular, he provides no details regarding the specific conduct by Sunbelt that amounts to "accessing, intercepting, monitoring, reviewing, storing and using [his] post-employment private electronic data and electronic communications." *Id.* He also fails to aver any facts to establish that Sunbelt's use of the intercepted communications was highly offensive. *See Folgelstrom*, 195 Cal.App.4th at 993, 125 Cal.Rptr.3d 260. The possibility that Sunbelt may have reviewed text messages sent to a cell phone which it owned and controlled—without more—is insufficient to establish an offensive use. As with his other claims, Victor's formulaic recitation of an invasion of privacy claim is inconsistent with the federal pleading requirements of Rule 8. This claim is DISMISSED with leave to amend.

IV. *CONCLUSION*

For the reasons stated above,

IT IS HEREBY ORDERED THAT:

1. Plaintiff's Motion to Dismiss Defendants Counterclaims is GRANTED.

2. Defendant shall have twenty-one (21) days from the date this Order is filed to amend his counterclaims, consistent with the Court's rulings. Defendant is warned that any factual allegations set forth in his amended pleading must be made in good faith and consistent with Rule 11. The failure to timely file the amended counterclaim and/or the failure to comply with this Order will result in the dismissal of all counterclaims with prejudice.

IT IS SO ORDERED.

N.D.Cal., 2014
Sunbelt Rentals, Inc. v. Victor
--- F.Supp.2d ----, 2014 WL 4274313 (N.D.Cal.), 2014 IER Cases 167,127

END OF DOCUMENT

830 F.Supp.2d 1083, Blue Sky L. Rep. P 74,956
(Cite as: 830 F.Supp.2d 1083)

C

United States District Court,
W.D. Washington,
at Seattle.
AVENTA LEARNING, INC., et al., Plaintiffs,
v.
K12, INC., et al., Defendants.

Case No. C10–1022JLR.
Nov. 8, 2011.

Background: Shareholders and former executives of acquired corporation filed state court suit against acquiring company and its parent, alleging violation of Washington State Securities Act (WSSA), misrepresentation, and breach of implied covenant of good faith and fair dealing, and sought equitable relief of constructive trust, injunction, or accounting. Acquiring company removed and counterclaimed for breach of separation agreement and conversion. Plaintiffs moved to dismiss counterclaims, and defendants moved for protective order and for summary judgment.

Holdings: The District Court, James L. Robart, J., held that:
(1) genuine issue of material fact as to when plaintiffs knew, or had reason to discover, alleged misrepresentations in asset purchase agreement (APA) precluded summary judgment on statute of limitations claims for WSSA violation and misrepresentation;
(2) APA, which provided for future payout, was not a "security" under WSSA;
(3) genuine issue of material fact as to whether representations in APA were materially misleading precluded summary judgment on misrepresentation claim;
(4) issues of material fact regarding acquiring company's discretion regarding accounting methods used to determine future payout precluded summary judgment on claim for breach of covenant of good faith and fair dealing;
(5) shareholders did not have standing to bring suit as individuals;
(6) defendant stated claim for breach of employment contract;
(7) defendant stated claim for breach of separation agreement;
(8) defendant stated claim for conversion of electronic files;
(9) employee waived attorney-client privilege he may have had to materials saved on his company-issued laptop by relinquishing it to his employer;
(10) vice president was charged with constructive knowledge of company's privacy policies; and
(11) employer's policy allowed it to access and disclose any file or stored communication on laptop.

Ordered accordingly.

West Headnotes

[1] Limitation of Actions 241 100(1)

241 Limitation of Actions
241II Computation of Period of Limitation
241II(F) Ignorance, Mistake, Trust, Fraud, and Concealment or Discovery of Cause of Action
241k98 Fraud as Ground for Relief
241k100 Discovery of Fraud
241k100(1) k. In general. Most Cited Cases

Under Washington law's discovery rule, cause of action for misrepresentation accrues for limitation purposes when plaintiff discovers or reasonably should have discovered essential elements of claim;

discovery rule does not require knowledge of existence of a legal cause of action.

[2] Limitation of Actions 241 95(2)

241 Limitation of Actions
241II Computation of Period of Limitation
241II(F) Ignorance, Mistake, Trust, Fraud, and Concealment or Discovery of Cause of Action
241k95 Ignorance of Cause of Action
241k95(2) k. Want of diligence by one entitled to sue. Most Cited Cases

Under Washington law's discovery rule, for purposes of accrual of cause of action, general rule is that when a plaintiff is placed on notice by some appreciable harm occasioned by another's wrongful conduct, plaintiff must make further diligent inquiry to ascertain scope of the actual harm.

[3] Limitation of Actions 241 104.5

241 Limitation of Actions
241II Computation of Period of Limitation
241II(G) Pendency of Legal Proceedings, Injunction, Stay, or War
241k104.5 k. Suspension or stay in general; equitable tolling. Most Cited Cases

Under Washington law, equitable tolling of statute of limitations is permitted where there is evidence of bad faith, deception, or false assurances by defendant and the exercise of diligence by plaintiff.

[4] Federal Civil Procedure 170A 2511

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2511 k. Securities cases in general. Most Cited Cases

Federal Civil Procedure 170A 2513

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2513 k. Corporations and business organizations. Most Cited Cases

Genuine issue of material fact as to when shareholders of acquired corporation knew, or had reason to discover, that financial projections contained in acquiring company's asset purchase agreement (APA) for corporation were allegedly inaccurate precluded summary judgment on acquiring company's claim that three year statute of limitations for violation of Washington State Securities Act (WSSA) and misrepresentation claim had run. West's RCWA 4.16.080(4), 21.20.430(4)(b).

[5] Securities Regulation 349B 248

349B Securities Regulation
349BII State Regulation
349BII(A) In General
349Bk248 k. Securities requiring registration or qualification in general. Most Cited Cases

The definition of “security” in Washington State Securities Act (WSSA) embodies a flexible rather than a static principle, one that is capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits. West's RCWA 21.20.005(12)(a) (2010).

[6] Securities Regulation 349B 248

349B Securities Regulation

349BII State Regulation
349BII(A) In General
349Bk248 k. Securities requiring registration or qualification in general. Most Cited Cases

Essential attribute of a "security," under Washington State Securities Act (WSSA), is an investment premised on a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others. West's RCWA 21.20.005(12)(a) (2010).

[7] Securities Regulation 349B 309

349B Securities Regulation
349BII State Regulation
349BII(B) Civil Effects of Violations
349Bk303 Actions
349Bk309 k. Trial and relief. Most Cited Cases

Under Washington State Securities Act (WSSA), whether or not an investment scheme or contract constitutes a security is a question of law. West's RCWA 21.20.005(12)(a) (2010).

[8] Securities Regulation 349B 248

349B Securities Regulation
349BII State Regulation
349BII(A) In General
349Bk248 k. Securities requiring registration or qualification in general. Most Cited Cases

In determining whether a transaction constitutes the sale of a security, under Washington State Securities Act (WSSA), court should consider substance over form, consistent with the purpose of the act to protect the investing public. West's RCWA 21.20.005(12)(a) (2010).

[9] Securities Regulation 349B 252

349B Securities Regulation
349BII State Regulation
349BII(A) In General
349Bk249 Particular Securities
349Bk252 k. Investment contracts. Most Cited Cases

In determining whether a transaction constitutes the sale of a security under Washington State Securities Act (WSSA), courts apply a modified *Howey* test which defines an "investment contract security" as: (1) an investment of money (2) in a common enterprise, and (3) efforts of promoter or a third party must have been fundamentally significant ones that affected the investment's success or failure. West's RCWA 21.20.005(12)(a) (2010).

[10] Securities Regulation 349B 248

349B Securities Regulation
349BII State Regulation
349BII(A) In General
349Bk248 k. Securities requiring registration or qualification in general. Most Cited Cases

For purposes of determining whether an investment is a "security" under Washington State Securities Act (WSSA), a "risk capital investment" may arise where investor does not receive the right to exercise practical and actual control over the managerial decisions of the venture. West's RCWA 21.20.005(12)(a) (2010).

[11] Securities Regulation 349B 252

349B Securities Regulation
349BII State Regulation
349BII(A) In General
349Bk249 Particular Securities
349Bk252 k. Investment contracts. Most Cited Cases

In determining whether a transaction constitutes the sale of a security under Washington State Securities Act (WSSA), courts in Washington, while recognizing that the risk capital definition is distinct from the definition of an investment contract, nevertheless appear to combine their analyses of both concepts under the *Howey* definition. West's RCWA 21.20.005(12)(a) (2010).

[12] Securities Regulation 349B 252

349B Securities Regulation
349BII State Regulation
349BII(A) In General
349Bk249 Particular Securities
349Bk252 k. Investment contracts. Most Cited Cases

Asset purchase agreement (APA), which provided that acquiring company would pay future cash earnout payment to executives of acquired corporation, was not a "security," pursuant to Washington State Securities Act (WSSA), utilizing either investment contract or risk capital formulation under modified *Howey* test, since executives themselves exercised practical or actual control over amount of future cash earnout payments they would receive; following execution of APA, executives became vice presidents of acquiring company, and as part of six-person executive team, they were responsible for strategic and operational decisions with respect to all business decisions affecting their eventual payout. West's RCWA 21.20.005(12)(a) (2010).

[13] Fraud 184 3

184 Fraud
184I Deception Constituting Fraud, and Liability Therefor
184k2 Elements of Actual Fraud
184k3 k. In general. Most Cited Cases

Under Washington law, to prevail on a claim for intentional misrepresentation, plaintiff must show: (1) representation of an existing fact; (2) materiality; (3) falsity; (4) speaker's knowledge of its falsity; (5) intent of speaker that it should be acted upon by plaintiff; (6) plaintiff's ignorance of its falsity; (7) plaintiff's reliance on truth of the representation; (8) plaintiff's right to rely upon the representation; and (9) damages suffered by plaintiff.

[14] Fraud 184 18

184 Fraud
184I Deception Constituting Fraud, and Liability Therefor
184k18 k. Materiality of matter represented or concealed. Most Cited Cases

Under Washington law, a "material" misrepresentation is one to which a reasonable person would attach importance when determining whether to participate in a transaction.

[15] Federal Civil Procedure 170A 2513

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2513 k. Corporations and business organizations. Most Cited Cases

In action involving asset purchase transaction between two educational learning companies, genuine issues of material fact as to whether acquiring company had made a material misrepresentation to acquired corporation in its models projecting future performance after acquisition, and whether it was reasonable for acquired corporation to rely on those projections, precluded summary judgment in acquired corporation's misrepresentation claim against acquir-

ing company.

[16] Contracts 95 168

95 Contracts
95II Construction and Operation
95II(A) General Rules of Construction
95k168 k. Terms implied as part of contract. Most Cited Cases

Under Washington law, the implied duty of good faith and fair dealing obligates parties to a contract to cooperate with each other so that each may obtain the full benefit of performance.

[17] Contracts 95 168

95 Contracts
95II Construction and Operation
95II(A) General Rules of Construction
95k168 k. Terms implied as part of contract. Most Cited Cases

Under Washington law, the implied duty of good faith and fair dealing prevents a contracting party from engaging in conduct that frustrates the other party's right to the benefits of the contract.

[18] Contracts 95 168

95 Contracts
95II Construction and Operation
95II(A) General Rules of Construction
95k168 k. Terms implied as part of contract. Most Cited Cases

Under Washington law, the covenant of good faith and fair dealing applies when a contract gives one party discretionary authority to determine a contract term; it does not apply to contradict contract terms.

[19] Federal Civil Procedure 170A 2513

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2513 k. Corporations and business organizations. Most Cited Cases

In action involving asset purchase agreement between two educational learning companies, genuine issue of material fact as to whether acquiring company had exercised its discretion with regard to accounting methods and other factors affecting the calculations of earnings before interest, taxes, depreciation and amortization (EBITDA), thereby affecting amount of future cash earnout payment executives of acquired corporation would receive under asset purchase agreement, precluded summary judgment in acquired corporation's claim for breach of covenant of good faith and fair dealing against acquiring company.

[20] Federal Civil Procedure 170A 2513

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2513 k. Corporations and business organizations. Most Cited Cases

In action involving asset purchase agreement between two educational learning companies, genuine issue of material fact as to what access acquired corporation had been given to acquiring company's information and documents relating to calculations of earnings before interest, taxes, depreciation and amortization (EBITDA), which, in turn, had affected amount of future cash earnout payment executives of acquired corporation received, precluded summary judgment on acquired corporation's claim for equita-

ble relief of constructive trust, accounting, or injunction.

[21] Corporations and Business Organizations 101 2029

101 Corporations and Business Organizations
101VIII Derivative Actions; Suing or Defending on Behalf of Corporation
101VIII(A) In General
101k2027 Persons Entitled to Sue or Defend; Standing
101k2029 k. Derivative or direct action. Most Cited Cases

Under Washington law, ordinarily, a shareholder cannot sue for wrongs done to a corporation, because corporation is viewed as a separate entity, and shareholder's interest is too remote to meet standing requirements.

[22] Corporations and Business Organizations 101 2029

101 Corporations and Business Organizations
101VIII Derivative Actions; Suing or Defending on Behalf of Corporation
101VIII(A) In General
101k2027 Persons Entitled to Sue or Defend; Standing
101k2029 k. Derivative or direct action. Most Cited Cases

Under Washington law, even a shareholder who owns all or most of corporation's stock, but who suffers damages only indirectly as a shareholder, cannot sue as an individual.

[23] Corporations and Business Organizations 101 2029

101 Corporations and Business Organizations
101VIII Derivative Actions; Suing or Defending on Behalf of Corporation
101VIII(A) In General
101k2027 Persons Entitled to Sue or Defend; Standing
101k2029 k. Derivative or direct action. Most Cited Cases

Under Washington law, there are two exceptions to rule that shareholder cannot sue for wrongs done to a corporation: (1) where there is a special duty, such as a contractual duty, between wrongdoer and shareholder; and (2) where shareholder suffered an injury separate and distinct from that suffered by other shareholders.

[24] Corporations and Business Organizations 101 2029

101 Corporations and Business Organizations
101VIII Derivative Actions; Suing or Defending on Behalf of Corporation
101VIII(A) In General
101k2027 Persons Entitled to Sue or Defend; Standing
101k2029 k. Derivative or direct action. Most Cited Cases

Under Washington law, exception to rule that shareholder cannot sue for wrongs done to a corporation unless there is a special duty, applies only when that special duty had its origin in circumstances independent of stockholder's status as a stockholder.

[25] Corporations and Business Organizations 101 2129

101 Corporations and Business Organizations
101VIII Derivative Actions; Suing or Defending on Behalf of Corporation
101VIII(C) Derivative Actions by Sharehold-

ers Against Third Parties
101k2127 Persons Entitled to Sue or Defend; Standing
101k2129 k. Derivative or direct action. Most Cited Cases

Corporations and Business Organizations 101 2728

101 Corporations and Business Organizations
101X Mergers, Acquisitions, and Reorganizations
101X(C) Sale, Lease, or Exchange of Substantially All Corporate Assets
101k2725 Actions
101k2728 k. Persons entitled to sue; standing. Most Cited Cases

Under Washington law, shareholders in acquired corporation could not bring suit individually against acquiring company for misrepresentation, based on its allegedly inaccurate financial projections in asset purchase agreement (APA), since corporation was express beneficiary under the APA, and there was no evidence that individual shareholders had suffered injury separate from their status as shareholders.

[26] Labor and Employment 231H 32

231H Labor and Employment
231HI In General
231Hk31 Contracts
231Hk32 k. In general. Most Cited Cases

Under Washington law, to state a claim for breach of employment contract, plaintiff must allege that contract imposed a duty, that duty was breached, and that breach proximately caused damages.

[27] Labor and Employment 231H 114(3)

231H Labor and Employment
231HIII Rights and Duties of Employers and Employees in General
231Hk109 Employee's Duties
231Hk114 Conflict of Interest
231Hk114(3) k. Other employers or similar parties. Most Cited Cases

Under Washington law, employer stated claim for breach of employment contract against its former employees by alleging that under contract employees had duty of fidelity and loyalty not to engage in competitive business for a defined period of time, duty not to interfere with its business relationships with clients, and duty to promptly return all of employer's property upon termination of their employment, that employees had failed to abide by these duties when they left employment to start a new company, and that employer had been injured by employees' actions.

[28] Contracts 95 312(4)

95 Contracts
95V Performance or Breach
95k312 Acts or Omissions Constituting Breach in General
95k312(4) k. Contract not to engage in or injure business carried on by another. Most Cited Cases

Under Washington law, employer stated claim for breach of separation agreement against its former employee by alleging that agreement prohibited tampering with or using employer's proprietary information following employee's termination and required employee to return employer's property, including copies of electronic materials, upon termination, and that employee had, without authorization, downloaded proprietary records onto electronic storage device or external hard drive following separation from the company.

[29] Conversion and Civil Theft 97C 100

97C Conversion and Civil Theft
97CI Acts Constituting and Liability Therefor
97Ck100 k. In general; nature and elements. Most Cited Cases

Under Washington law, elements of conversion are an unjustified, willful interference with a chattel which deprives a person entitled to the property of possession.

[30] Conversion and Civil Theft 97C 111

97C Conversion and Civil Theft
97CI Acts Constituting and Liability Therefor
97Ck110 Detention of Property
97Ck111 k. In general. Most Cited Cases

Conversion and Civil Theft 97C 115

97C Conversion and Civil Theft
97CI Acts Constituting and Liability Therefor
97Ck115 k. Use or disposition of property. Most Cited Cases

Conversion and Civil Theft 97C 117

97C Conversion and Civil Theft
97CI Acts Constituting and Liability Therefor
97Ck117 k. Destruction of or injury to property. Most Cited Cases

Washington courts look to the Restatement (Second) of Torts when analyzing conversion claims, which recognizes claims for conversion in variety of circumstances, including wrongfully detaining chattel, destroying or altering chattel, exceeding the authorized use of chattel, and misusing chattel. Restatement (Second) of Torts §§ 221–241.

[31] Conversion and Civil Theft 97C 112

97C Conversion and Civil Theft
97CI Acts Constituting and Liability Therefor
97Ck110 Detention of Property
97Ck112 k. Possession or control. Most Cited Cases

Under Washington law, employer stated claim for conversion against its former employees by alleging that they had copied, accessed, and destroyed proprietary electronic files, thus wrongfully detaining and exceeding authorized use of the files, and thereby had deprived employer of its rightful possession or control; even though employer still had access to original files, it did not mean that it was not deprived of employees' copies of the files.

[32] Privileged Communications and Confidentiality 311H 102

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk102 k. Elements in general; definition. Most Cited Cases

Privileged Communications and Confidentiality 311H 137

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk135 Mode or Form of Communications
311Hk137 k. Documents and records in general. Most Cited Cases

Under Washington law, attorney-client privilege applies to confidential communications and advice between an attorney and client and extends to documents that contain a privileged communication.

[33] Privileged Communications and Confidentiality 311H 173

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk171 Evidence
311Hk173 k. Presumptions and burden of proof. Most Cited Cases

Under Washington law, party asserting attorney-client privilege has burden of proving all elements of the privilege, including the absence of waiver.

[34] Privileged Communications and Confidentiality 311H 168

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk168 k. Waiver of privilege. Most Cited Cases

Under Washington law, employee waived any attorney-client privilege he may have had to materials saved on his company-issued laptop when, following separation from his employment, he relinquished laptop to his employer; at time of relinquishment, employee failed to assert any type of attorney-client privilege as to any of the materials on the laptop or take any precautions to protect the privacy of the materials saved there, so he no longer had any reasonable expectation of confidentiality with regard to the information.

[35] Corporations and Business Organizations 101 1847

101 Corporations and Business Organizations
101VII Directors, Officers, and Agents
101VII(D) Rights, Duties, and Liabilities as to Corporation and Its Shareholders or Members
101k1840 Fiduciary Duties as to Management of Corporate Affairs in General
101k1847 k. Duty to inquire; knowledge or notice. Most Cited Cases

Privileged Communications and Confidentiality 311H 141

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk135 Mode or Form of Communications
311Hk141 k. E-mail and electronic communication. Most Cited Cases

Under Washington law, for purposes of determining attorney-client privilege of material contained on employer-issued laptop, even if vice president of educational learning company had never been provided with an employee handbook outlining the company's policies concerning privacy of electronic communications, he was charged with constructive knowledge of the material contained therein, since, as a senior level manager, he was expected to know company policies in order to properly manage and supervise employees.

[36] Privileged Communications and Confidentiality 311H 156

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk156 k. Confidential character of communications or advice. Most Cited Cases

Under Washington law, only confidential communications between an attorney and a client are protected; for attorney-client privilege to apply, client must have a reasonable expectation that the communications are confidential and will be kept confidential.

[37] Privileged Communications and Confidentiality 311H 141

311H Privileged Communications and Confidentiality

311HIII Attorney-Client Privilege
311Hk135 Mode or Form of Communications
311Hk141 k. E-mail and electronic communication. Most Cited Cases

Privileged Communications and Confidentiality 311H 156

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk156 k. Confidential character of communications or advice. Most Cited Cases

Under Washington law, materials vice president of educational learning company had saved or stored on his company-issued laptop, including emails sent and received which consisted of privileged attorney-client communications, and materials which had been created prior to his employment, were not protected by attorney-client privilege, since he had no reasonable expectation that the materials were confidential and would be kept confidential; laptop was not his property, and pursuant to company policy, company reserved right to access and disclose any file or stored communication on the device at any time, including web-based personal email accounts accessed through employer-issued computer or laptop.

[38] Privileged Communications and Confidentiality 311H 141

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk135 Mode or Form of Communications
311Hk141 k. E-mail and electronic communication. Most Cited Cases

Privileged Communications and Confidentiality 311H 168

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk168 k. Waiver of privilege. Most Cited Cases

Under Washington law, in evaluating whether an employee has waived attorney-client privileged status of personal communications transmitted, stored, or saved onto a company computer or laptop, court considers whether: (1) company maintained a policy banning personal or other objectionable use; (2) company monitored the use of employee's computer or email; (3) third parties had right of access to computer or emails; and (4) company notified employee, or employee was aware, of the policy.

***1089** Michael A. Goldfarb, Christopher M. Huck, Kelley Donion Gill Huck & Goldfarb, PLLC, Seattle, WA, for Plaintiffs.

Ronald L. Berenstain, Sean C. Knowles, Perkins Coie, Steven P. Caplow, Davis Wright Tremaine, Seattle, WA, Sarah J. Crooks, Perkins Coie, Portland, OR, for Defendants.

ORDER ON MOTIONS FOR SUMMARY JUDGMENT, FOR DISMISSAL OF COUNTERCLAIMS, AND FOR PROTECTIVE ORDER

JAMES L. ROBART, District Judge.

I. INTRODUCTION

Before the court are three motions: (1) Plaintiffs Micheal J. Axtman and James J. Benitez's motion to dismiss Defendant KC Distance Learning, Inc.'s ("KCDL") counterclaims (Dkt. # 58); (2) Defendants K12, Inc. ("K12"), Kayleigh Sub Two LLC, and KCDL's motion for a protective order (Dkt. # 61); and (3) KCDL's motion for summary judgment (Dkt. # 81). K12, Inc. and Kayleigh Sub Two LLC have joined in KCDL's motion for summary judgment. (Joinder (Dkt. # 84).) Having reviewed the motions, and all materials filed in support and opposition thereto, and having heard the oral argument of counsel concerning the motion for summary judgment and the motion to dismiss on November 3, 2011,[FN1] the court

GRANTS IN PART and DENIES IN PART KCDL's motion for summary judgment, DENIES Mr. Axtman and Mr. Benitez's motion to dismiss KCDL's counterclaims,[FN2] and GRANTS Defendants' motion for a protective order.

FN1. No party requested oral argument or a hearing with regard to Defendants' motion for a protective order, and the court deems the declarations and other papers submitted by the parties to be sufficient for purposes of its ruling.

FN2. On November 2, 2011, Defendants voluntarily dismissed counterclaims four and five for breach of the duty of loyalty and for misrepresentation, respectively. (Dkt. # 100.) Accordingly, the court denies Plaintiffs' motion to dismiss these two counterclaims as moot.

II. FACTUAL AND PROCEDURAL BACKGROUND

A. Background Related to Defendants' Motion for Summary Judgment

Plaintiff Aventa Learning, Inc. ("Aventa") is a Washington corporation founded in 2002 by Mr. Axtman and Mr. Benitez. (Am. Compl. (Dkt. # 26) ¶¶ 1, 4, 9.) Aventa assists schools in bringing their educational curricula online. (*Id.* ¶ 4.) The individual plaintiffs, Mr. Axtman, Mr. Benitez, Dr. Ronald P. Benitez, Elizabeth A. Benitez, Robert E. Harbison, and Susanne M. Harbison are the sole shareholders in Aventa. (*Id.* ¶ 5.)

Mr. Axtman and Mr. Benitez remain the president and secretary of Aventa, respectively. (Knowles Decl. (Dkt. # 82) Ex. C (Axtman Dep.) at 7:10–77:24.) Prior to cofounding Aventa, Mr. Benitez was employed as a corporate finance analyst at an investment banking firm. (*Id.* Ex. B (Benitez Dep.) at 207:1–5, 207:25–208:2.) In addition, both men were previously employed at Apex Learning, which is an online education company. (*Id.* Ex. B (Benitez Dep.) at 212:16–213:9; Ex. C (Axtman Dep.) at 20:10–18.) At Apex, Mr. Axtman was responsible for creating business projections. (*Id.* Ex. C. at 20:10–18.)

KCDL is a provider of distance learning programs. Pursuant to an Asset Purchase Agreement ("APA"), dated January 10, 2007, KCDL acquired substantially all of the assets of Aventa. (Knowles Decl. Ex. M.) Knowledge Learning Corporation ("KLC") acquired KCDL as part of a larger acquisition of another company. (*Id.* ***1090** Ex. A ("Brown Dep.") at 20:7–21:10.) After the acquisition, KLC hired Stephen Brown as the Chief Executive Officer of KCDL with the intent to expand KCDL. (*Id.*) In the fall of 2006, Mr. Brown began negotiating with Mr. Axtman and Mr. Benitez regarding the acquisition of Aventa by KCDL. (*See id.* Ex. H.)

KCDL regularly developed five-year financial projection models as part of its annual budgeting process. (*Id.* Ex. D. (Solis Dep.) at 68:15–24, 71:20–72:10.) The models include projections of revenues by business line, costs, expenses, net income, gross margin, and Earnings Before Interest, Taxes, Depreciation, and Amortization ("EBITDA") for each of the five subsequent fiscal years. (*See id.* Ex. L at KCDL011986.) On October 19, 2006, Mr. Brown responded by email to Aventa's request for KCDL's EBITDA projections, stating that KCDL projected 2009 EBITDA of $16 million and 2011 of $37 million. (*Id.* Ex. I at KCDL001348.) These projections were taken from an August 2006 EBITDA model that reflected an assumption that KCDL would acquire Aventa ("the August 2006 Buy Model"). (*Id.* Ex. A ("Brown Dep.") at 70:18–71:6, 71:10–16; Ex. F at KCDL014499; Ex. G at KCDL034319.)

On November 30, 2006, Mr. Brown emailed Mr. Axtman and Mr. Benitez two five-year models dated October 20, 2006, one reflecting financial projections assuming that KCDL would acquire Aventa'a assets

(the "October 2006 Buy Model"), and another reflecting financial projections assuming that KCDL would not. (*Id.* Ex. L.) The October Buy Model contained revenue projections for each of KCDL's lines of business by year from 2007 through 2011 and projected total EBITDA for that period to be $86 million. (*Id.* at KCDL011986.) While the August 2006 Buy Model projected EBITDA for 2009 and 2011 to be $16 million and $37 million, respectively, the October 2006 Buy Model projected EBITDA for 2009 and 2011 to be $12 million and $41 million, respectively. (Knowles Decl. Ex. I at KCDL001348; Ex. L at KCDL011986.) Nevertheless, Mr. Brown told Mr. Axtman that the numbers changed only because Mr. Brown had incorporated the new Aventa numbers (which Mr. Axtman and Mr. Benitez had previously provided) into the October 2006 Buy Model. (*See* Goldfarb Decl. (Dkt. # 86) Ex. F (Axtman Dep.) at 139:18–143:11.)

On January 10, 2007, KCDL, Aventa and the individual Plaintiffs executed the APA. (*Id.* Ex. N.) The APA provides consideration to Aventa for the sale of its assets to KCDL, as follows: (1) $2.34 million at closing; (2) the "Aventa Earnout," worth up to $3.3 million, based primarily on the 2007 performance of Aventa's assets; and (3) the "Additional Earnout," a future payment equal to "six percent (6%) of the Assumed Equity Value" of KCDL at a certain future point. (*Id.* at KCDL115629–34; Axtman Decl. (Dkt. # 87) Ex. H(APA) § 2.03(c)(i).) The Assumed Equity Value for calculating the Additional Earnout was to be derived by taking KCDL's trailing 12–month period EBITDA and applying a multiplier that increased based on the number of years that Mr. Axtman and Mr. Benitez served as senior executives of KCDL after the transaction. (Knowles Decl. Ex. N at PLTF000051–53.)

Aventa received $2.34 million at closing and $3.3 million pursuant to the Aventa Earnout in 2008. (Knowles Decl. Ex. C (Axtman Dep.) at 166:16–18, 167:9–15; Ex. B (Benitez Dep.) at 147:23–148:3, 148:13–149:4.) KCDL has place an additional $1.7 million in escrow, representing its calculation of the Additional Earnout, pending resolution of this lawsuit. (Knowles Decl. ¶¶ 23, 25.) Further, in connection with the ***1091** APA, or about January 12, 2007, Mr. Axtman and Mr. Benitez each executed an employment agreement with KCDL. (Answer (Dkt. # 55) ¶ 13.)

On February 15, 2007, Mr. Axtman and Mr. Benitez received an updated 5–year model dated February 9, 2007 ("the February 2007 Model"). (Knowles Decl. Exs. O, P; C (Axtman Dep.) 181:16–25; Ex. B (Benitez Dep.) 153:4–16.) In this model, KCDL's total projected EBITDA for the five-year period from 2007 through 2011 was $45 million (Knowles Decl. Ex. P at KCDL020018–9), which was significantly less than the $86 million projected EBITDA total for the same period reflected in the October 2006 Buy Model (*id.* Ex. L at KCDL011986).

Shortly after receiving the February 2007 Model, Mr. Axtman testifies that he spoke with Mr. Brown who reassured him that the numbers in the February 2007 Model were artificially low, and that the accurate model was still the "October 2006 Buy Model." (Goldfarb Decl. (Dkt. # 86) Ex. F (Axtman Decl.) at 184:5–189:8.) Mr. Axtman also passed Mr. Brown's reassurances onto Mr. Benitez. (*Id.* at 185:19–23;) *see also* Axtman Decl. Ex. F at KCDL019950 (describing February 2007 Model to Mr. Benitez as "a sandbag.")

As contemplated in the APA, immediately after the asset purchase closed, Mr. Axtman and Mr. Benitez joined KCDL as Vice Presidents in charge of KCDL's Aventa Learning business line. (Knowles Decl. Ex. C (Axtman Dep.) 170:11–24; Ex. B. (Benitez Dep.) 150:24–151:1.) Mr. Axtman and Mr. Benitez immediately became members of the senior executive team and participated in weekly senior staff meetings with Mr. Brown and other senior executives. (*Id.* Ex. C (Axtman Dep. at 171:1–20); Ex. B. (Benitez Dep.) at 151:2–19; Ex. A. (Brown Dep.) at

262:8–263:12.) Mr. Axtman and Mr. Benitez also became involved in other aspects of KCDL's business. They prepared financial projections and 5–year models and participated in KCDL's budgeting process. (*Id.* Ex. A (Brown Dep.) 263:13–264:3, 265:23–266:7, 268:16–24; Ex. Q; Ex. C (Axtman Dep.) 195:1–196:14; Ex. B (Benitez Dep.) at 179:12–180:6, 187:11–21; Ex. D (Solis Dep.) 245:20–246:10.) In October 2008, Mr. Axtman joined KCDL's Board of Directors. (*Id.* Ex. C (Axtman Dep.) 205:8–25.) In early 2009, Mr. Axtman became the head of the iQ Academies business line at KCDL. (*Id.*)

On July 26, 2010, K12 announced that it had purchased KCDL. (Am. Compl. ¶ 39.) The sale of KCDL constituted a "change of control" transaction under the APA allowing KCDL to elect to pay the Additional Earnout. (Knowles Decl. ¶ 23; Ex. M at KCDL115633.) Aventa disputed KCDL's calculation and demanded access to KCDL's books, records, and facilities. (*Id.* ¶ 24.) On January 19, 2011, KCDL paid $1.7 million as the Additional Earnout payment into an escrow account pending resolution of this lawsuit. (*Id.* ¶¶ 23, 25.) On March 14, 2011, KCDL provided Aventa with its response to the dispute, as well as approximately 50,000 pages of records. (*Id.* ¶ 26.)

Plaintiffs initiated this lawsuit on June 2, 2010. Plaintiffs allege violation of the Washington State Securities Act ("WSSA"), RCW 21.20 *et seq.* (Am. Compl. ¶¶ 43–50), the tort of misrepresentation (*id.* ¶¶ 51–60), breach of the implied covenant of good faith and fair dealing (*id.* ¶¶ 61–66), a claim for declaratory relief (*id.* ¶¶ 67–69), and entitlement to equitable relief such as a constructive trust over Aventa's assets, an injunction, or an accounting (*id.* ¶¶ 70–74). Defendants have moved for summary judgment with regard to all of Plaintiffs' claims. (SJ Mot. (Dkt. # 81).)

***1092 B. Background Related to Motion to Dismiss**

In their answer to Plaintiffs' amended complaint, Defendants assert counterclaims against Mr. Axtman and Mr. Benitez. (KCDL Answer (Dkt. # 55) at 13–22, ¶¶ 1–69 (Counterclaims).) Defendants' allegations arise in connection with the employment agreements executed by Mr. Axtman and Mr. Benitez, and their eventual separation from KCDL. (*Id.* ¶¶ 13–26.) Defendants allege that the employment agreements at issue contained loyalty, non-compete, and non-interference clauses. (*Id.* ¶¶ 14–17.) Defendants also allege that the employment agreements required Mr. Axtman and Mr. Benitez to return all property, records, and other files at the end of their employment that Mr. Axtman or Mr. Benitez had prepared for or received from KCDL during their employment. (*Id.* ¶ 18.) In addition to his employment agreement, Defendants allege that Mr. Axtman executed a separation agreement with KCDL and KCL. (*Id.* ¶¶ 19–22.)

Defendants allege that, prior to and following his separation from KCDL, Mr. Axtman formed and promoted a new company to compete with KCDL, that Mr. Axtman interfered with KCDL's clients, and that he improperly accessed proprietary information belonging to KCDL. (*Id.* ¶¶ 23–26.) They also allege the Mr. Benitez improperly accessed KCDL's proprietary information. (*Id.* ¶ 26.)

Based on these factual allegations, Defendants assert six counterclaims. Defendants assert that both Mr. Axtman and Mr. Benitez breached their employment agreements with KCDL. (*Id.* ¶¶ 27–34, 40–45.) They assert that Mr. Axtman breached his separation agreement with KCDL by copying, deleting, and destroying records and proprietary information that were on the KCDL laptop that was in his possession following the termination of his work relationship with KCDL. (*Id.* ¶¶ 35–39.) They also allege that both Mr. Axtman and Mr. Benitez breached their duty of loyalty to KCDL (*id.* ¶¶ 46–54), committed the tort of misrepresentation (*id.* ¶¶ 55–63), and converted KCDL's property by accessing, copying, downloading, deleting or erasing KCDL's electronic records following the termination of their employment (*id.* ¶¶ 64–69). Plaintiffs have moved to dismiss each of these counterclaims. (Mot. to Dismiss (Dkt. # 58).)

830 F.Supp.2d 1083, Blue Sky L. Rep. P 74,956
(Cite as: 830 F.Supp.2d 1083)

C. Background Related to Motion for Protective Order

As a part of the APA, both Mr. Axtman and Mr. Benitez signed employment agreements with KCDL. (KCDL Answer at 14, ¶ 13 (Counterclaims).) [FN3] KCDL subsequently issued both men laptop computers. (Axtman Decl. re: P.O. (Dkt. # 68) ¶ 6; Benitez Decl. re: P.O. (Dkt. # 69) ¶ 6.) Both men transferred privileged attorney-client communications that had been created prior to their employment ***1093** with KCDL onto their new laptop computers. (*See* Axtman Decl. re: P.O. ¶¶ 3–4, 8–9; Benitez Decl. re: P.O. 3–4, 8–9.) Both men have testified that they stored these files locally on their laptops, and did not believe that their local files were transferred to KCDL's or KLC's servers.[FN4] (Axtman Decl. re: P.O. ¶ 12; Benitez Decl. re: P.O. ¶ 12.) Both men also continued to produce attorney-client privileged communications in the form of emails on their work laptops after execution of the APA and the commencement of their employment at KCDL. (*Id.*)

FN3. Defendants now assert that "[Mr.] Benitez and [Mr.] Axtman were employed by KLC and assigned to KCDL." (Mot. for P.O. (Dkt. # 61) at 2 (citing 1st Keegan Decl. (Dkt. # 63) ¶ 2).) Both Mr. Benitez and Mr. Axtman deny that they were ever employed by KLC, and insist that they were only employed by KLC's subsidiary KCDL. (Axtman Decl. re: P.O. (Dkt. # 68) ¶ 5; Benitez Decl. re: P.O. (Dkt. # 69) ¶ 5; *see generally* Sur-reply (Dkt. # 74).) Indeed, Mr. Axtman and Mr. Benitez have moved (as part of their sur-reply) to strike portions of Defendants' reply that that asserts that Mr. Axtman's and Mr. Benitez's employment agreements with KCDL did not accurately reflect their employer or relationship with KCDL. (Sur-reply at 2.) The court, however, does not believe that the dispute is material for purposes of this motion, because it is undisputed that "KLC performed the complete human resources function for KCDL, including administration of all benefits, employee relations, and policy promulgation." (1st Keegan Decl. (Dkt. # 63) ¶ 2.)

FN4. Despite this belief, some of these materials were in fact transferred at some point onto Defendants' servers. (*See* P.O. Mot. (Dkt. # 61) at 1; P.O. Reply (Dkt. # 70) at 4.)

KLC performs the human resources function for KDLC.[FN5] (1st Keegan Decl. (Dkt. # 63) ¶ 2.) This function includes administration of all benefits, employer relations, and policy promulgation. (*Id.*) KLC also provides technology services for KCDL, including email. (*Id.*)

FN5. Although Mr. Axtman and Mr. Benitez both deny that they were ever employed by KLC, neither has disputed that KLC performed the human services function for KDLC during the period of their employment, including the promulgation of company policies.

KLC has an Employee Handbook governing it and its subsidiaries and affiliates that contains an Electronic Communications Policy that provides, in part:

> All resources used for electronic communications are KLC property and should generally be used only for KLC business.
>
> * * *
>
> Electronic communications are not private. KLC reserves the right to access, search, inspect, monitor, record, and disclose any file or stored communication, with or without notice to the employee, at any time for any reason to ensure that such communi-

cations are being used for legitimate business reasons. Deleted e-mail messages may also be restored from the system.

(1st Keegan Decl. ¶ 3, Ex. 2 at 21.)[FN6] KLC regularly enforces this policy. (*Id.* ¶ 5.) Employees' laptops have been reviewed by the company, and employees have been disciplined, including having their employment terminated, for violations. (*Id.*)

FN6. KLC also has a second, more detailed, policy entitled the Electronic Communications and Computer Usage Policy. (1st Keegan Decl. ¶ 4, Ex. 3.) This policy is set forth on KLC's intranet site, which is known as KLCentral. (2nd Keegan Decl. (Dkt. # 72) ¶ 4.) Defendants provided testimony that Mr. Benitez and Mr. Axtman had access and were granted logins to KLCentral, and as senior managers were expected to know the contents of company policies that were set forth on KLCentral. (*Id.* ¶¶ 4–5.) Nevertheless, both Mr. Axtman and Mr. Benitez testified that they did not use or access KLCentral, and were not aware of and did not review the Electronic Communications and Computer Usage Policy on KLCentral. (Axtman Decl. re: P.O. ¶ 14; Benitez Decl. re P.O. ¶ 14.) In addition, Mr. Benitez testified that he "do[es] not believe [he] was even provided a username and password to access KLCentral." (*Id.*) As a result of this factual dispute concerning Mr. Benitez's ability to even access KLCentral, the court does not consider the Electronic Communications and Computer Usage Policy in its analysis of the privilege issues, but rather confines its analysis to the Electronic Communications Policy contained within the company handbook.

Defendants have produced testimony that it is the pattern and practice of KLC to provide all employees, including those assigned to its affiliates and subsidiaries, with copies of the Employee Handbook upon hiring, and that (in accord with this policy and practice) Mr. Axtman and Mr. Benitez would have received this Handbook upon the commencement of their employment.***1094** (*Id.* ¶ 6; *see also* 2nd Keegan Decl. (Dkt. # 72) ¶ 3.)

Mr. Axtman and Mr. Benitez, however, have both testified that to the best of their knowledge they never received copies of KLC's employee handbook, and were not aware of KLC's policies prior to their transfer of privileged files onto their KCDL laptops. (Axtman Decl. re: P.O. ¶ 13; Benitez Decl. re: P.O. ¶ 13.) In addition, Defendants have not produced copies of "Employee Acknowledgements" signed by either Mr. Axtman or Mr. Benitez concerning their receipt of KLC's policies or its handbook.

Nevertheless, Defendants have produced a copy of a template letter from Mr. Brown that was sent to all Aventa Employees who were being retained by KCDL following execution of the APA by Aventa and KCDL. (*See* 1st Keegan Decl. ¶ 6, Ex. 4.) The letter specifically instructs the new KCDL employees from Aventa to review the employee handbook. (*Id.* Ex. 4 at 2.) Neither Mr. Axtman nor Mr. Benitez specifically deny receiving a copy of this letter. (*See generally* Benitez Decl. & Axtman Decl.) Further, the letter directs the new employees to contact Mr. Axtman with any questions concerning the transition. (*Id.* Ex. 4 at 3.)

Despite Mr. Axtman's and Mr. Benitez's inability to specifically recall receiving a copy of the KLC Handbook (*see* Axtman Decl. re: P.O. ¶ 13; Benitez Decl. re: P.O. ¶ 13), there can be no doubt that Mr. Benitez received a copy by at least November 19, 2007, and that both men received a copy by February 23, 2009. Defendants have produced a copy of a November 19, 2007 email to a new hire at KCDL, on which Mr. Benitez was copied, and which attaches a copy of the KLC Handbook. (2nd Keegan Decl. Ex. 1.) The email describes the KLC Handbook as the

employee handbook, and specifically asks the new KCDL hire to review it with regard to company policies. (*Id.*) Mr. Benitez does not specifically deny receiving this email. (*See generally* Benitez Decl.) Further, Defendants have produced a copy of a February 23, 2009 email addressed to both Mr. Axtman and Mr. Benitez, which also attaches the KLC Handbook. (2nd Keegan Decl. Ex. 2.) Neither Mr. Axtman nor Mr. Benitez has specifically denied receiving this email. (*See generally* Axtman Decl. & Benitez Decl.)

After his employment with KCDL ended, Mr. Axtman returned his laptop to the company in late 2009. He did not, however, make a claim with regard to any privileged documents contained on his laptop until May 12, 2011, nearly a year and half after he relinquished the laptop to the company. (Crooks Decl. (Dkt # 62) ¶¶ 7–8, Ex. 5.)

Mr. Benitez was terminated on September 28, 2010, but initially refused to return his company laptop. He asserted that he had saved years worth of privileged communications on his laptop. Counsel for Defendants asserted that Mr. Benitez had no expectation of privacy with regard to contents on the laptop, and insisted that he return it because it was company property. (Crooks Decl. Ex. 1.) Mr. Benitez ultimately returned the laptop on January 21, 2011 (*id.* ¶ 3), but only after Defendants had agreed to a "review protocol" that would require Defendants to sequester the asserted privileged material prior to reviewing the remainder of the laptop's contents (*id.* Ex. 2).

The emails or other documents at issue in this motion include asserted privileged communications (1) from before execution of the APA in January 2007, which Mr. Benitez and Mr. Axtman saved on their KCDL laptops in a folder in Microsoft Outlook (which was a program provided by the company), (2) from Mr. Axtman's and Mr. Benitez's web-based personal email ***1095** accounts, which they saved and imported into Microsoft outlook on their KCDL laptops, and (3) from Mr. Axtman's and Mr. Benitez's post-acquisition work email accounts, which they saved in Microsoft Outlook on their KCDL laptops. In addition, Plaintiffs assert that some of these privileged materials may be residing on Defendants' computers and servers. Defendants seek a protective order from the court declaring that these documents are not privileged and/or that the privilege has been waived.

III. ANALYSIS

A. Motion for Summary Judgment

1. Standards

Defendants have moved for summary judgment of all claims against them in Plaintiffs' amended complaint. (*See* SJ Mot.) Summary judgment is appropriate if the evidence, when viewed in the light most favorable to the non-moving party, demonstrates "that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed.R.Civ.P. 56(a); *see Celotex Corp. v. Catrett*, 477 U.S. 317, 322, 106 S.Ct. 2548, 91 L.Ed.2d 265 (1986); *Galen v. Cnty. of L.A.*, 477 F.3d 652, 658 (9th Cir.2007). The moving party bears the initial burden of showing there is no genuine issue of material fact and that he or she is entitled to prevail as a matter of law. *Celotex*, 477 U.S. at 323, 106 S.Ct. 2548. If the moving party meets his or her burden, then the non-moving party "must make a showing sufficient to establish a genuine dispute of material fact regarding the existence of the essential elements of his case that he must prove at trial" in order to withstand summary judgment. *Galen*, 477 F.3d at 658.

2. Statute of Limitations

Defendants assert that the three-year statute of limitations has run with regard to Plaintiffs' WSSA and misrepresentation claims. They argue that Plaintiffs' claims under the WSSA and for misrepresentation are based on their allegations that the financial projections and EBITDA calculations contained in the October 2006 Buy Model were false or misleading. They further assert, however, that Mr. Axtman and Mr. Benitez had notice of their claims no later than

February 2007, and therefore, Plaintiffs' claims, which were filed in June 2010, are time-barred.

There is no dispute that Mr. Axtman and Mr. Benitez received three sets of financial projections between October 2006 and February 2007—all of which are dramatically different from one another. Defendants assert that the receipt of these varying financial projections and EBITDA calculations placed Plaintiffs on notice that the October 2006 Buy Model was false or misleading. The statute of limitations for a WSSA claim is three years from the date on which the violation was or could have been discovered in the exercise of reasonable care. RCW 21.20.430(4)(b). In addition, causes of action for misrepresentation must be brought within three years and accrue when the aggrieved party has discovered the facts constituting misrepresentation. *See* RCW 4.16.080(4) (three-year statute of limitations for fraud); *Young v. Savidge*, 155 Wash.App. 806, 230 P.3d 222, 230 (Wash.Ct.App.2010) (applying statute of limitations from RCW 4.16.080(4) to claims for misrepresentation).

[1][2] A cause of action accrues when the plaintiff knew or should have known all the facts underlying the essential elements of the action. *Reichelt v. Johns–Manville Corp.*, 107 Wash.2d 761, 733 P.2d 530, 534 (1987); *1000 Virginia Ltd. Partnership v. Vertecs Corp.*, 158 Wash.2d 566, 146 P.3d 423, 428 (2006). In Washington, the general rule is that when a plaintiff is placed on notice by some appreciable harm occasioned by another's wrongful conduct, the plaintiff must make further diligent inquiry***1096** to ascertain the scope of the actual harm. *Green v. A.P.C.*, 136 Wash.2d 87, 960 P.2d 912, 916 (1998). It is not necessary for the plaintiff to be aware that he has a legal cause of action. *Reichelt*, 733 P.2d at 534–35. But an injured plaintiff who reasonably suspects that a specific wrongful act has occurred is on notice that legal action must be taken. *Id.* at 534. The plaintiff is charged with what a reasonable inquiry would have discovered. *Green*, 960 P.2d at 916.

[3] Washington, however, allows equitable tolling of the statute of limitations when justice requires. *Thompson v. Wilson*, 142 Wash.App. 803, 175 P.3d 1149, 1154 (Wash.Ct.App.2008); *see also Stueckle v. Sceva Steel Buildings, Inc.*, 1 Wash.App. 391, 461 P.2d 555, 557 (Wash.Ct.App.1970) ("The statute of limitations may be tolled by the concealment of material facts, misrepresentation, or a promise to pay in the future."). "Equitable tolling is permitted where there is evidence of bad faith, deception or false assurances by the defendant and the exercise of diligence by the plaintiff." *Thompson*, 175 P.3d at 1154; D. DeWolf, K. Allen & D. Caruso, 25 Wash. Prac. § 16.19 (2010) ("Washington recognizes an equitable tolling principle....").

[4] Plaintiffs assert that after receiving the October 2006 Buy Model, Mr. Brown reassured them that the differences between the projections in this model and the projections in the August 2006 Buy Model were due to the inclusion of the new Aventa numbers into the October 2006 Buy Model. (*See* Goldfarb Decl. Ex. F (Axtman Dep.) at 139:18–143:11.) Plaintiffs further contend that after receiving the February 2007 Model, Mr. Brown again reassured them that the numbers in the February 2007 Model were artificially low, and that the accurate model was still the October 2006 Buy Model. (*Id.* at 184:5–189:8.) On this summary judgment motion, the court must view the evidence in the light most favorable to Plaintiffs. Applying this standard, and taking into account the reassurances issued by Mr. Brown, the court cannot conclude that reasonable minds could not differ as to the commencement of the running of the statute of limitation in February 2007 or the tolling of the statute by Mr. Brown's reassurances concerning the differences in the various models Plaintiffs' received. These are material issues of fact which must be reserved for the jury. Accordingly, the court denies Defendants' motion for summary judgment with regard to the statute of limitations.

830 F.Supp.2d 1083, Blue Sky L. Rep. P 74,956
(Cite as: 830 F.Supp.2d 1083)

3. Plaintiffs' WSSA Claim

Defendants contend that neither the sale of Aventa's assets to KCDL nor the Additional Earnout under the APA constitute a security under Washington law, and therefore, Plaintiffs' WSSA claim must fail. (SJ Mot. at 12–18.) Although the court previously rejected Defendants' argument in this regard in the context of their motion to dismiss (*see* Order (Dkt. # 54) at 11–18), Defendants have raised the issue again here on summary judgment.

There are two essential elements to a WSSA claim: "(1) a fraudulent or deceitful act committed (2) in 'connection with the offer, sale or purchase of any security.' " *Kinney v. Cook*, 159 Wash.2d 837, 154 P.3d 206, 209–10 (2007) (quoting RCW 21.20.010).[FN7] It is the second prong of this ***1097** test that is once again at the heart of the present dispute.

FN7. It is unlawful for any person, in connection with the offer, sale or purchase of any security, directly or indirectly:

(1) To employ any device, scheme, or artifice to defraud;

(2) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they are made, not misleading; or

(3) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person.

RCW 21.20.010.

[5][6] WSSA broadly defines a "security," in pertinent part, as follows:

"Security" means any ... stock; ... investment contract; investment of money or other consideration in the risk capital of a venture with the expectation of some valuable benefit to the investor where the investor does not receive the right to exercise practical and actual control over the managerial decisions of the venture; ... or, in general, any interest or instrument commonly known as a "security"....

RCW 21.20.005(12)(a). "[T]he definition of security 'embodies a flexible rather than a static principle, one that is capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits.' " *Cellular Eng'g, Ltd. v. O'Neill*, 118 Wash.2d 16, 820 P.2d 941, 946 (1991) (quoting *SEC v. W.J. Howey*, 328 U.S. 293, 299, 66 S.Ct. 1100, 90 L.Ed. 1244 (1946)). However, "[t]he essential attribute of a security is an investment 'premised on a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others.' " *Firth v. Lu*, 103 Wash.App. 267, 12 P.3d 618, 623 (Wash.Ct.App.2000) (quoting *United Housing Found. v. Forman*, 421 U.S. 837, 852, 95 S.Ct. 2051, 44 L.Ed.2d 621 (1975)).

[7][8] Whether or not an investment scheme or contract constitutes a security is a question of law. *Swartz v. Deutsche Bank*, No. C03–1252MJP, 2008 WL 1968948, at *22 (W.D.Wash. May 2, 2008) (citing *De Luz Ranchos Inv. Ltd. v. Coldwell Banker & Co.*, 608 F.2d 1297, 1299–1301 (9th Cir.1979)); *see also Haberman v. Washington Pub. Power Supply Sys.*, 109 Wash.2d 107, 744 P.2d 1032, 1047 (1987) ("[W]e note that federal courts consistently determine as a matter of law whether investment schemes are securities.") (citing cases).[FN8] In determining whether a transaction constitutes the sale of a security, the court should consider substance over form, consistent with the purpose of the act to protect the investing public. *Cellular Eng'g*, 820 P.2d at 946.

FN8. "... Washington courts have looked to federal law in determining whether a transaction involves a 'security.' " *Shinn v. Thrust IV, Inc.*, 56 Wash.App. 827, 786 P.2d 285, 298 (Wash.Ct.App.1990) (citing *State v. Philips*, 108 Wash.2d 627, 741 P.2d 24, 28 (1987)); *see also* RCW 21.20.900 (policy of the WSSA is to make uniform the law and to coordinate its interpretations and administration with related federal regulation).

[9] Defendants assert that the issue of whether the APA or the Additional Earnout is a security should be analyzed under the test for an "investment contract" as stated in *Howey*, 328 U.S. at 301, 66 S.Ct. 1100. (SJ Mot. at 13.) Washington courts apply a modified *Howey* test which defines an "investment contract" security as "(1) an investment of money (2) in a common enterprise and (3) the efforts of the promoter or a third party must have been fundamentally significant ones that affected the investment's success or failure." *Ito Int'l Corp. v. Prescott, Inc.*, 83 Wash.App. 282, 921 P.2d 566, 571–72 (Wash.Ct.App.1996); *see also Cellular Eng'g*, 820 P.2d at 946. The third prong of the modified *Howey* test looks to whether the profits on an enterprise "come 'primarily' or 'substantially' from the efforts of others." *Id.* at 946 (citing *Sec. & Exch. Comm'n v. Glenn W. Turner Enters., Inc.*, 474 F.2d 476, 482 (9th Cir.1973)). Defendants assert that Plaintiffs fail to satisfy the third element of this test.

***1098** [10][11] Although Plaintiffs defend their position that the Additional Earnout is a security under the "investment contract" analysis (*see* SJ Resp. (Dkt. # 85) at 12–17), they also argue that the Additional Earnout constitutes a security under the "risk capital" formulation that is also contained within the statutory definition (*see id.* at 11–12 (citing RCW 21.20.005(12)(a))).[FN9] "A risk capital investment may arise 'where the investor does not receive the right to exercise practical and actual control over the managerial decisions of the venture.' " *Ultimate Timing, LLC v. Simms*, No. C08–1632–MJP, 2010 WL 2650705, at *2 (W.D.Wash. June 29, 2010) (citing *Sauve v. K.C., Inc.*, 91 Wash.2d 698, 591 P.2d 1207 (1979) (applying an earlier version of RCW 21.20.005(12) that did not include "risk capital," but describing a risk capital investment as one "with a reasonable expectation of a valuable benefit but without the right to control the enterprise.")). Courts in Washington, while recognizing that "the risk capital definition is distinct from the definition of an investment contract," nevertheless "appear to combine their analyses of both concepts under the *Howey* definition." *Ultimate Timing*, 2010 WL 2650705, at *2 (citing *Ito Int'l*, 921 P.2d at 571). One court has declared: "Adoption of the 'risk capital' approach ... does not obviate the *Howey* test that has heretofore been applied by the Washington courts." *State v. Philips*, 45 Wash.App. 321, 725 P.2d 627, 630 (Wash.Ct.App.1986).

FN9. Plaintiffs also assert that the Additional Earnout constitutes a security because certain federal regulations and courts treat "phantom stock" or a stock appreciation right ("SAR") as a security, and prior to the execution of the APA, Mr. Axtman and Mr. Benitez were promised a "phantom equity interest" in KCDL and certain KCDL officers characterized the transaction as providing Plaintiffs with "phantom stock," "a phantom SAR plan," or "phantom equity" in KCDL. (*See* SJ Resp. at 9–11.) Nowhere does the APA itself refer to "phantom stock," "phantom equity," or "phantom SARs." In deciding whether a security is at issue here, the court must look to the substance or realities of the transaction. *Sauve v. K.C., Inc.*, 91 Wash.2d 698, 591 P.2d 1207, 1208 (Wash.Ct.App.1979) ("In determining whether a given transaction constitutes a 'security' within the meaning of these statutes, form should be disregarded for substance, and the emphasis should be on

> economic reality.") Accordingly, the court is less concerned with the informal nomenclature used by various parties either before or after the transaction, and more concerned with the actual terms of the APA. Further, Plaintiffs have failed to provide one case in which a court has concluded that an asset purchase agreement, which includes the type of future cash earnout payment at issue here, constitutes the purchase of a security. Accordingly, the court concludes that the proper analysis is to consider the APA and its Additional Earnout under the modified *Howey* test or the "rick capital" formulation.

A recent decision in the Western District of Washington, interpreting Washington law on this issue, is instructive. In *Ultimate Timing,* 2010 WL 2650705, plaintiff made an investment in an enterprise devoted to the commercialization and marketing of a race timing system in exchange for a 20% ownership and profit interest in the enterprise. *Id.* at *2. The plaintiff, however, conceded that he "spent substantial time and effort marketing the timing system to race directors and race timers during the time he was working with [the company]." *Id.* He also negotiated on behalf of the company. *See Ultimate Timing, LLC v. Simms,* 715 F.Supp.2d 1195, 1209 (W.D.Wash.2010). The *Ultimate Timing* court found that under either the "risk capital" or the "investment contract" analysis of "security," the plaintiff's own description of the investment required dismissal of the claim. *Ultimate Timing,* 2010 WL 2650705, at *2. The court found that the plaintiff's "capital contribution was not an investment contract because [the company's] profitability turned on [the ***1099** plaintiff's] own ability to market the system to timers and races." *Id.* The court also found that the plaintiff's capital contribution "[l]ikewise ... was not a 'risk capital investment' because [the plaintiff] exercised practical or actual control over the entity." *Id.*

[12] Like the result in *Ultimate Timing,* the result here is also the same under either the "investment contract" or "risk capital" formulation. There is no dispute that immediately following the execution of the APA, both Mr. Axtman and Mr. Benitez joined KCDL as Vice Presidents in charge of KCDL's Aventa Learning business line. (*See* Knowles Decl. Ex. C (Axtman Dep.) at 170:11–24l; Ex. B (Benitez Dep.) at 150:24–151:1.) Indeed, Mr. Axtman's and Mr. Benitez's employment agreements are attached as exhibits to the APA and require that they become "Vice President[s], Sales" immediately after the transaction. (Knowles Decl. Ex. N at PLTF000054.) In addition, there is no dispute that Mr. Axtman and Mr. Benitez became members of KCDL's six-person executive team, which was responsible for strategic and operational decisions with respect to all of KCDL's business, immediately after the transaction closed in January 2007. (Knowles Decl. Ex. A (Brown Dep.) at 262:18–263:12.)

Mr. Axtman and Mr. Benitez try to minimize these significant contributions by asserting that they did not have the authority to hire and fire employees (SJ Resp. at 12), although Mr. Benitez admitted that immediately after the transaction, he and Mr. Axtman "could hire a sales team." (2nd Knowles Decl. (Dkt. # 93) Ex. B (Benitez Dep.) at 88:16–89:10.) They also try to minimize their involvement by asserting that they traveled for work extensively promoting sales or worked from home. (SJ Resp. at 12.) However, both testified that they did in fact typically participate in weekly executive meetings—albeit via telephone. (2nd Knowles Decl. Ex. B (Benitez Dep.) at 151:12–19; Ex. C (Axtman Dep.) at 171:1–20.) In any event, in this day and age of almost ubiquitous connectivity via cellular telephones and laptop computers, the court finds Mr. Axtman's and Mr. Benitez's travel schedules or the location of their remote offices to be immaterial with regard to the significance of their contributions to company management. Indeed, the court finds that the involvement of Mr. Benitez and Mr. Axtman to be at least as significant, if not more so, than the plaintiff in *Ultimate Timing*. Accordingly, the

court finds that neither the APA nor the Additional Earnout meets the definition of either an investment contract or a risk capital investment, and accordingly is not a security under the WSSA. Defendants are entitled to summary judgment on Plaintiffs' WSSA claim, and the court dismisses the claim.

4. Plaintiffs' Misrepresentation Claim

[13][14] "In order to prevail on a claim for intentional misrepresentation, [the plaintiff] must show: '(1) representation of an existing fact, (2) materiality, (3) falsity, (4) the speaker's knowledge of its falsity, (5) intent of the speaker that it should be acted upon by the plaintiff, (6) plaintiff's ignorance of its falsity, (7) plaintiff's reliance on the truth of the representation, (8) plaintiff's right to rely upon the representation, and (9) damages suffered by the plaintiff.' " *Poulsbo Group, LLC v. Talon Dev., LLC,* 155 Wash.App. 339, 229 P.3d 906, 909–10 (Wash.Ct.App.2010) (quoting *W. Coast, Inc. v. Snohomish Cnty.*, 112 Wash.App. 200, 48 P.3d 997, 1000 (Wash.Ct.App.2002)). A material misrepresentation is one to which a reasonable person would attach importance when determining whether to participate in a transaction. *Aspelund v. Olerich,* 56 Wash.App. 477, 784 P.2d 179, 183 (Wash.Ct.App.1990). "Each element must be established by ***1100** 'clear, cogent and convincing evidence.' " *Id.* (quoting *Stiley v. Block,* 130 Wash.2d 486, 505, 925 P.2d 194, 200 (Wash.1996)). Defendants assert that Plaintiffs have failed to prove by the necessary evidentiary standard (1) the existence of a material false representation, and (2) their right to rely upon it. (SJ Mot. at 18–21.)

[15] Plaintiffs' misrepresentation claim arises out of Defendants' presentation to them of certain models (such as the October 2006 Buy Model, and others described above) projecting the performance of KCDL following its acquisition of Aventa. The heart of Plaintiffs' misrepresentation claim is the allegation that Defendants presented the October 2006 Buy Model as a good-faith estimate of KCDL's EBITDA, when in fact it was not generated in good faith. (Am. Compl. ¶ 33.) As noted above, the standard of proof for an intentional misrepresentation claim is high, and may prove to be a hurdle too high for Plaintiffs to clear at trial. The court, nevertheless, finds that given the disputed nature of the testimony concerning the methods used to develop the various models received by Mr. Axtman and Mr. Benitez both before and after execution of the APA, conflicting testimony concerning the rigor underpinning these models and their reliability or lack thereof, as well as Defendants' and other witnesses' various statements to Plaintiffs about these models, Plaintiffs have raised sufficient material factual issues regarding the existence of a false representation to survive summary judgment.

With regard to the issue of Plaintiffs' right to rely upon the alleged misrepresentations, the court finds Plaintiffs have raised sufficient material factual issues to survive summary judgment on this issue, as well. The reliance issue is not, as Defendants assert, whether Plaintiffs were entitled to rely on the projections as a "guarantee of future performance" (SJ Mot. at 21)—clearly they were not. Rather, the issue is whether they were entitled to rely upon Defendants' representations about the rigor of the analysis underpinning the models—for example, that the projections were reasonable, based on fair assumptions or methodology, and supported by a significant capital plan.

Further, contrary to Defendants' assertions, Plaintiffs were not required to make further inquiry once Defendants had made representations or reassurances to Plaintiffs concerning the rigor of the models. "A party to whom a positive, distinct and definite representation has been made is entitled to rely on that representation and need not make further inquiry concerning the particular facts involved." *Douglas Nw., Inc. v. Bill O'Brien & Sons Constr., Inc.,* 64 Wash.App. 661, 828 P.2d 565, 577 (1992); *see also ABN Amro Mortg. v. Greene,* No. C04–0450C, 2005 WL 2207027, at *3 (W.D.Wash. Aug. 10, 2005) (applying Washington law). This rule is applied if the misrepresentations are made to induce conduct, the

misrepresentations succeed in inducing conduct, and the complaining party was actually deceived and mislead by the misrepresentations. *Jenness v. Moses Lake Dev. Co.*, 39 Wash.2d 151, 234 P.2d 865, 869 (1951) (quoting *Cunningham v. Studio Theatre, Inc.*, 38 Wash.2d 417, 229 P.2d 890, 894 (1951)). When applying this rule, "it is immaterial that the means of knowledge are open to the complaining party, or easily available to him, and that he may ascertain the truth by proper inquiry or investigation." *Jenness*, 234 P.2d at 869 (quoting *Cunningham*, 229 P.2d at 894). Accordingly, the court denies Defendants' motion for summary judgment on Plaintiffs' misrepresentation claim.

5. Duty of Good Faith and Fair Dealing Claim

[16][17] The implied duty of good faith and fair dealing "obligates parties [to a contract] to cooperate with each other so ***1101** that each may obtain the full benefit of performance." *Badgett v. Sec. State Bank*, 116 Wash.2d 563, 807 P.2d 356, 360 (1991). The duty prevents a contracting party from engaging in conduct that frustrates the other party's right to the benefits of the contract. *Woodworkers of Am. v. DAW Forest Prods. Co.*, 833 F.2d 789, 795 (9th Cir.1987). Plaintiffs' claim for breach of the duty of good faith and fair dealing is based on allegations that KCDL, through it management bonus plan and certain accounting methods, artificially suppressed EBITDA generation, which undermined and limited Plaintiffs' expected compensation under the Additional Earnout.[FN10] (Am. Compl. ¶¶ 61–66.)

FN10. "[T]he APA provides that the Additional Earnout is calculated based on a percentage of, 'equal to six percent (6%) of the Assumed Equity Value' of KCDL." (Am. Compl. ¶ 18 (quoting APA § 2.03(c)).) "Assumed Equity Value" is in turn based on KCDL's EBITDA. (*Id.* ¶ 27; Knowles Decl. Ex. M(APA) § 203(c).)

Although Defendants acknowledge that Washington courts recognize an implied duty of good faith and fair dealing in every contract, *see Betchard–Clayton, Inc. v. King*, 41 Wash.App. 887, 707 P.2d 1361, 1364 (Wash.Ct.App.1985), they correctly assert that the duty of good faith and fair dealing "does not extend to obligate the party to accept a material change in the terms of its contract," nor "inject substantive terms into the parties' contract." *Badgett*, 807 P.2d at 360 (internal citations and quotation marks omitted). Accordingly, they move to dismiss Plaintiffs' claim on summary judgment, arguing that no provision of the APA requires KCDL to maximize EBITDA. (SJ Mot. at 22.)

[18] The issue, however, is not the injection of a substantive term into the APA, but rather whether KCDL exercised its discretion with regard to accounting methods and other factors affecting the calculation of EBITDA following execution of the APA in good faith. "The covenant of good faith applies when the contract gives one party discretionary authority to determine a contract term; it does not apply to *contradict* contract terms." *Goodyear Tire & Rubber Co. v. Whiteman Tire, Inc.*, 86 Wash.App. 732, 935 P.2d 628, 632 (Wash.Ct.App.1997) (italics in original). As stated by the court:

> The duty of good faith and fair dealing applies when one party has discretionary authority to determine certain terms of the contract, such as quantity, price, or time.... The covenant may be relied upon only when the manner of performance under a specific contract term allows for discretion on the part of either party.... However, it will not contradict terms or conditions for which a party has bargained.

Id. (quoting *Amoco Oil Co. v. Ervin*, 908 P.2d 493, 498 (Colo.1995)); *see also Craig v. Pillsbury Non–Qualified Pension Plan*, 458 F.3d 748, 752 (8th Cir.2006) ("Ordinary contract principles require that, where one party is granted discretion under the terms of the contract, that discretion must be exercised in good faith—a requirement that includes the duty to

exercise the discretion reasonably.") (applying Washington law).

[19] Under the APA, Plaintiffs' Additional Earnout was based, in part, on KCDL's calculation of its EBITDA. The determination of EBITDA is not an exact science, and can be affected by a range of accounting and other factors within Defendants' discretion. Plaintiffs presented evidence that following execution of the APA, KCDL implemented certain accounting policy changes that suppressed its EBITDA calculation. (*See* Goldfarb Decl. Ex. P (Beaton Supp. Expert Report) ¶ 31(a)-(e).) For example, certain KCDL employees questioned the value received for shared services charged to KCDL by KLC, which ***1102** reduced EDITDA. (*Id.* ¶ 31(e); Benitez Decl. Ex. E at KCDL086560; Goldfarb Decl. Ex. S at 15.) While Defendants submit evidence that KCDL revised its bonus plan to incentivize the maximization of EBITDA (Cogan Decl. (Dkt. # 83)),[FN11] this evidence does not negate the existence of a material issue of fact in light of the evidence presented by Plaintiffs. Accordingly, the court denies Defendants' motion for summary judgment on this issue.[FN12]

FN11. In their opposition to Defendants' motion for summary judgment, Plaintiffs move to strike Mr. Cogan's declaration on grounds that KCDL did not disclose Mr. Cogan as an expert witness in any of its Federal Rule of Civil Procedure 26(a) initial disclosures, even though KCDL had supplemented those disclosures only one month prior to filing its motion for summary judgment. (SJ Resp. at 23–24.) Because the court has denied Defendants' motion for summary judgment on this issue even in light of Mr. Cogan's declaration, Plaintiffs' request to strike Mr. Cogan's declaration is moot. Further, KCDL has stated that Plaintiffs were permitted the opportunity to depose Mr. Cogan prior to filing their response to KCDL's motion for summary judgment (SJ Reply (Dkt. # 92) at 12 n. 8 (citing 2nd Knowles Decl. ¶ 6)), and thus prejudice, if any, would appear to be minimal. In any event, the court's decision with regard to Mr. Cogan's declaration here does not preclude Plaintiffs from raising the issue of the admissibility of Mr. Cogan's testimony at trial in a motion in limine, if appropriate.

FN12. The APA provides that, if KCDL and Aventa cannot resolve any dispute concerning the calculation of the Additional Earnout payment, they shall submit the dispute to an independent accounting firm for "final, binding and conclusive" resolution. (Knowles Decl. Ex. M at KCDL115634.) In their motion for summary judgment, Defendants assert, in a one-sentence argument, that the APA requires arbitration before an independent accounting firm regarding any dispute over KCDL's calculation of the Additional Earnout. (SJ Mot. at 22.) In addition, Defendants address the issue in one sentence and a footnote within their reply memorandum. (SJ Reply at 12 & n. 9.) Likewise, Plaintiffs addressed the issue in three sentences within a footnote of their responsive memorandum. (SJ Resp. at 23, n. 4.) The court finds the parties' discussion of the issue wholly inadequate for purposes of any determination, and declines to consider this issue based on the sparse "briefing" provided by the parties. *See, e.g.*, *Indep. Towers of Wash. v. Wash.*, 350 F.3d 925, 929 (9th Cir.2003) ("As the Seventh Circuit observed in its now familiar maxim, '[j]udges are not like pigs, hunting for truffles buried in briefs.' ") (quoting *United States v. Dunkel*, 927 F.2d 955, 956 (7th Cir.1991)).

6. Claim for Declaratory Relief

[20] Defendants have moved for summary judgment of Plaintiffs' claim for declaratory relief.

Plaintiffs contend that they have been denied "reasonable access to KCDL's information and documents relating to EBITDA and the booking of transactions effecting EBITDA." (Am. Compl. ¶ 68.) Defendants assert that the claim should be dismissed on summary judgment because:

> ... KCDL provided Aventa with financial and accounting information to permit it to investigate the basis for the dispute. Aventa has received the information to which it is entitled pursuant to the APA.

(SJ Mot. at 23.) Defendants assert this bald statement without a scintilla of factual support. By way of contrast, Plaintiffs have submitted evidence of a continuing dispute concerning the adequacy of Defendants' production of documents and information as required under the APA relating to KCDL's calculation of EBITDA. (SJ Resp. at 24 (citing Goldfarb Decl. Exs. T, U).) The court, accordingly, denies Defendants' motion for summary judgment on this issue.

7. Individual Plaintiffs

[21][22][23][24] Defendants assert that the claims of the individual plaintiffs—Aventa's shareholders—should be dismissed because ***1103** the individual plaintiffs lack standing. A plaintiff must have a personal stake in the outcome of the case to bring suit. *Gustafson v. Gustafson,* 47 Wash.App. 272, 734 P.2d 949, 952 (Wash.Ct.App.1987). "Ordinarily, a shareholder cannot sue for wrongs done to a corporation, because the corporation is viewed as a separate entity, and the shareholder's interest is too remote to meet the standing requirements." *Id.* at 953. "Even a shareholder who owns all or most of the stock, but who suffers damages only indirectly as a shareholder, cannot sue as an individual." *Sabey v. Howard Johnson & Co.,* 101 Wash.App. 575, 5 P.3d 730, 735 (Wash.Ct.App.2000). There are two exceptions to this rule: "(1) where there is a special duty, such as a contractual duty, between the wrongdoer and the shareholder; and (2) where the shareholder suffered an injury separate and distinct from that suffered by other shareholders." *Id.* The special duty must have "its origin in circumstances independent of the stockholder's status as a stockholder." *Hunter v. Knight, Vale & Gregory,* 18 Wash.App. 640, 571 P.2d 212, 216 (Wash.Ct.App.1977).

[25] With regard to the first exception, Defendants assert that there is no evidence that they owed any special duty to the individual plaintiffs—independent of their status as stockholders of Aventa, and Plaintiffs have asserted none. (*See* SJ Resp. at 24.) With regard to the second exception, Defendants argue that although the individual plaintiffs signed the APA, they did so expressly in their capacity as shareholders of Aventa (Knowles Decl. Ex. M at KCDL115666–68), providing certain representations and warranties to KCDL (*see id.* at KCDL115636–48 (Articles III & IIIA)). Plaintiffs have not disputed these facts. Further, Plaintiffs have provided no evidence that the individual plaintiffs suffered any injury separate and distinct from those allegedly suffered by Aventa. The claims they assert are identical to those asserted by Aventa, and any injury they have allegedly incurred arises by virtue of their status as an Aventa shareholder.

Earlier in these proceedings, the court declined to dismiss the claims of the individual plaintiffs on Defendants' motion to dismiss. (Order (Dkt. # 54) at 9–10.) As the court noted in its prior ruling, however, neither party had cited any authority for its position. (*Id.* at 9.) Further, the posture of the case and the standards guiding the court were obviously different in the context of Defendants' motion to dismiss. The court now finds that Defendants have met their initial burden of showing that they are entitled to prevail on this issue as a matter of law, and Plaintiffs have failed to demonstrate a genuine issue of material fact in response.[FN13] Accordingly, the court grants Defendants' motion for summary judgment dismissing the claims of the individual plaintiffs.[FN14]

FN13. In its earlier order denying dismissal of the individual plaintiffs, the court relied on *Far West Fed. Bank v. Office of Thrift Supervision–Director*, 119 F.3d 1358, 1363–64 (9th Cir.1997). On summary judgment, it is apparent that the factual circumstances here are not in accord with *Far West*. In *Far West*, the written agreement at issue explicitly identified the individual investors as intended beneficiaries. *Id.* at 1364 & n. 2. In addition, there was evidence that breach of the contract would inflict injury upon the investors personally because they were induced by the defendant's promises to recapitalize the plaintiff thrift to the tune of tens of millions of dollars prior to execution of the agreement between the thrift and defendants. Here, the individual plaintiffs are not express beneficiaries under the APA, nor have plaintiffs provided evidence of individualized injury—separate from their status as Aventa's shareholders.

FN14. The court notes that although it is dismissing the claims of the individual plaintiffs on summary judgment, both Mr. Axtman and Mr. Benitez remain parties to this lawsuit as defendants to KCDL's cross-claims. Because Mr. Axtman and Mr. Benitez are no longer plaintiffs in this matter, they now would be properly viewed as third-party defendants to KCDL's claims. The court directs the parties to revise the caption in this matter so that it accurately reflects Mr. Axtman's and Mr. Benitez's current status in this litigation.

***1104 B. Motion to Dismiss Counterclaims**

1. Standards

The same standards applicable on a motion to dismiss a plaintiff's claim apply when considering a motion to dismiss a defendant's counterclaim. *See, e.g., In re Wash. Mut., Inc. Secs., Derivative & ERISA Litig.*, No. 08–MD–1919 MJP, 2011 WL 1158387, at *3 (W.D.Wash. Mar. 25, 2011). To survive a motion to dismiss, the counterclaim must have "facial plausibility [which exists] when the pleaded factual content allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 129 S.Ct. 1937, 1940, 173 L.Ed.2d 868 (2009). In reviewing the counterclaim, the court must assume the facts to be true and construe them in the light most favorable to the nonmoving party. *Cervantes v. United States*, 330 F.3d 1186, 1187 (9th Cir.2003).

2. Counterclaims One and Three—Alleged Breach of Employment Contract by Mr. Axtman and Mr. Benitez

[26][27] To state a counterclaim for breach of contract, KCDL must allege that the employment contracts between itself and Mr. Axtman and Mr. Benitez, respectively, impose a duty, that the duty has been breached, and that the breach proximately caused damages to KCDL. *Nw. Indep. Forest Mfrs. v. Dep't of Labor & Indus.*, 78 Wash.App. 707, 899 P.2d 6, 9 (Wash.Ct.App.1995). KCDL has adequately alleged that the employment contracts impose duties upon Mr. Axtman and Mr. Benitez, including (1) a duty of fidelity and loyalty to KCDL (KCDL Answer ¶¶ 14–15 (Counterclaims)), (2) a duty not to engage in any competitive business for a defined period of time (*id.* ¶ 16), (3) a duty not to interfere with KCDL's business relationships with its clients (*id.* ¶ 17), and (4) a duty to maintain all of KCDL's records and files prepared for or received from KCDL as the sole and exclusive property of KCDL, to not copy KCDL materials, and to promptly return to KCDL upon termination of their employment relationship all property belonging to KCDL (*id.* ¶ 18).

KCDL has also adequately alleged breach of the employment contracts by both men. KCDL has alleged that both Mr. Axtman and Mr. Benitez copied and destroyed proprietary information belonging to KCDL (*id.* ¶¶ 29–30, 44), that Mr. Axtman intention-

ally interfered with KCDL's business relationship with a client (*id.* ¶¶ 31–32), and that Mr. Axtman's plan to launch a new company that competed with KCDL and his incorporation of that company, violated the employment contract (*id.* ¶¶ 23, 33). KCDL has also adequately alleged damages with regard to these claims. (*Id.* ¶¶ 34, 45.) Plaintiffs' assertions that KCDL was not damaged by these alleged breaches or that Mr. Axtman's new company never actually competed with KCDL may be arguments more appropriate for summary judgment, but they do not succeed here on a motion to dismiss. Defendants' allegations with regard to counterclaims one and three are sufficient under the applicable standards recited above. Accordingly, the court denies Plaintiffs' motion to dismiss counterclaims one and three.

3. Counterclaim Two—Alleged Breach of the Separation Agreement by Mr. Axtman

[28] Plaintiffs assert that Defendants have failed to state a claim for breach of Mr. Axtman's separation agreement with KCDL on the basis of Mr. Axtman's copying of KCDL proprietary information following***1105** his separation from the company because the separation agreement does not prohibit the copying of documents. (Mot. to Dismiss at 7–8.) KCDL, however, has alleged that the contract prohibits tampering with or using KCDL proprietary information following termination of Mr. Axtman's work relationship. (*See* KCDL Answer ¶¶ 21, 36 (Counterclaims).) Further, KCDL has alleged that the Separation Agreement required Mr. Axtman to return all KCDL property, including copies of electronic materials (*id.* ¶ 22), and that, irrespective of these requirements, Mr. Axtman downloaded KCDL records onto an electronic storage device or external hard drive following his separation from the company (*id.* ¶ 25). Accordingly, KCDL has properly alleged breach of the separation agreement based on Mr. Axtman's copying of KCDL's files. The court denies Plaintiffs' motion to dismiss counterclaim two.

4. Counterclaim Six—Conversion

[29][30] Under Washington law, the elements of conversion are an unjustified, willful interference with a chattel which deprives a person entitled to the property of possession. *Potter v. Wash. State Patrol*, 165 Wash.2d 67, 196 P.3d 691, 696 (2008). The plaintiff must also plead that it has some property interest in the goods allegedly converted. *Coto Settlement v. Eisenberg*, 593 F.3d 1031, 1039 (9th Cir.2010) (citing *Meyers Way Dev. Ltd. Partnership v. Univ. Sav. Bank*, 910 P.2d 1308, 1320 (1996)). Washington courts look to the Restatement (Second) of Torts when analyzing conversion claims. *See, e.g.*, *Brown ex rel. Richards v. Brown*, 157 Wash.App. 803, 239 P.3d 602, 611 (Wash.Ct.App.2010) (citing and quoting the Restatement (Second) of Torts § 223 cmt. b (1965)). The Restatement recognizes claims for conversion in variety of circumstances, including wrongfully detaining chattel, destroying or altering chattel, exceeding the authorized use of chattel, and misusing chattel. *See* Restatement (Second) of Torts §§ 221–241.

[31] Plaintiffs assert that Defendants' counterclaim for conversion should be dismissed because simply accessing KCDL's files or copying them does not deprive KCDL of possession of the original electronic records remaining in KCDL's possession. (*See* Mot. to Dismiss at 14.) However, the court finds that KCDL's allegations that Mr. Axtman and Mr. Benitez copied, accessed, and destroyed KCDL's electronic files constitute "wrongfully detaining," "exceeding the authorized use of," or "misusing" those files, thereby depriving KCDL of its possession or control over such files. The fact that KCDL has access to another copy of the files at issue does not mean that it was not deprived of its possession of the copies accessed, made, or destroyed by Plaintiffs. Further, the court can find no logical basis for distinguishing between theft of copy and theft of the original electronic document. After all, the copy of the original (although allegedly created by Plaintiffs) would belong to Defendants as well. Courts dealing with this issue have begun to update the tort of conversion so that it keeps pace with

the contemporary realities of widespread computer use. *See, e.g.*, *E.I. DuPont de Nemours and Co. v. Kolon Indus., Inc.*, 688 F.Supp.2d 443, 455 (E.D.Va.2009) ("[Plaintiff's] claim for conversion, even if based exclusively on the transfer of copies of electronic information, survives [defendant's] motion to dismiss."); *Thyroff v. Nationwide Mut. Ins. Co.*, 8 N.Y.3d 283, 832 N.Y.S.2d 873, 864 N.E.2d 1272 (2007) ("[T]he tort of conversion must keep pace with the contemporary realities of widespread computer use," and therefore, "electronic records that [are] stored on a computer ... [are] subject to a claim of conversion ...."). The court denies ***1106** Plaintiffs' motion to dismiss counterclaim six for conversion.

C. Motion for Protective Order

[32][33] KCDL asserts in its motion for a protective order that Mr. Axtman and Mr. Benitez have waived any privilege with regard to attorney-client communications that they saved onto their KCDL laptop computers. Because this court's jurisdiction is based on diversity [FN15] and the underlying claims are predicated on state law, the privilege issues are governed by state law. *See* Fed.R.Evid. 501 ("[I]n civil actions and proceedings, with respect to an element of a claim or defense as to which State law supplies the rule of decision, the privilege of a ... person ... shall be determined in accordance with State law."); *In re Cal. Pub. Utils. Comm'n*, 892 F.2d 778, 781 (9th Cir.1989) ("In diversity actions, questions of privilege are controlled by state law."). Washington's attorney-client privilege applies to confidential communications and advice between an attorney and client and extends to documents that contain a privileged communication. *State v. Perrow*, 156 Wash.App. 322, 231 P.3d 853, 855 (Wash.Ct.App.2010). In Washington, the party asserting the attorney-client privilege has the burden of proving all the elements of privilege, including the absence of waiver. *See Dietz v. Doe*, 131 Wash.2d 835, 935 P.2d 611, 618–19 (1997); *see also Perrow*, 231 P.3d at 856. Mr. Axtman and Mr. Benitez bear the burden of proving that the attorney-client privilege attached to the communications at issue, and that they did not waive the attorney-client privilege with regard to materials that they accessed and saved on their KCDL laptop computers.

FN15. KCDL removed this action from King County Superior Court to this court on the basis of diversity jurisdiction. (Am. Compl. ¶ 2.)

1. Mr. Axtman's Laptop

[34] Washington courts have held that "[w]hen a client reveals information to a thirdparty, the attorney-client privilege is waived unless the third-party is necessary for the communication or has retained the attorney for a common interest." *Zink v. City of Mesa*, 162 Wash.App. 688, 256 P.3d 384, 403 (Wash.Ct.App.2011) (citing *Morgan v. City of Fed. Way*, 166 Wash.2d 747, 213 P.3d 596, 601 (2009)). Following his separation from KCDL, Mr. Axtman returned his laptop to the company in late 2009. He did not, however, assert the attorney-client privilege with regard to any documents contained on the laptop until May 12, 2011, nearly a year and half following his relinquishment of the computer. (Crooks Decl. ¶¶ 7–8, Ex. 5.) Once Mr. Axtman relinquished the laptop to KCDL (a third-party outside of his attorney-client relationship) without asserting privilege or taking any precautions to protect the privacy of materials that he had saved on the laptop, he no longer had any reasonable expectation of confidentiality with regard to those materials. Accordingly, under Washington law, he waived any privilege that may have been applicable. *See Zink*, 256 P.3d at 403; *Morgan*, 213 P.3d at 601. Such waiver would encompass all of the materials he placed or saved from any source onto his KCDL laptop computer. His belated attempt to assert the attorney-client privilege approximately a year and a half later is futile. Any privilege that may have existed with regard to these materials was extinguished by his unconditional relinquishment of the laptop and cannot be subsequently resurrected. Accordingly, the court grants Defendants' motion with regard to documents that Mr. Axtman saved onto his KCDL laptop

computer, and that may now be ***1107** stored on either his laptop or on Defendants' servers.

2. Mr. Benitez's Laptop

The court's analysis of both waiver and whether the attorney-client privileged ever attached to certain communications or materials that Mr. Benitez saved on his KCDL laptop stands on different grounds. Unlike Mr. Axtman, Mr. Benitez did not relinquish his KCDL laptop to the company without first asserting attorney-client privilege over certain materials contained on it, and without securing a sequestration agreement with regard to those materials from KCDL. The question with regard to Mr. Benitez's assertion of privilege is whether, in light of KCDL's policies concerning the use of its laptop computers by its employees, Mr. Benitez had any reasonable expectation of privacy with regard to attorney-client communications he saved on his laptop, or whether the act of saving those communications onto his KCDL laptop served to waive any privilege that may have existed.

As discussed above, KLC performs the human resource functions for KDLC, including policy promulgation. (1st Keegan Decl. (Dkt. # 63) ¶ 2.) Although both Mr. Benitez and Mr. Axtman have denied ever being employed by KLC as opposed to KDLC (Axtman Decl. re: P.O. ¶ 5; Benitez Decl. re: P.O. ¶ 5), neither has denied KLC's human resources role with regard to KDLC. Further, although Mr. Benitez testifies that "to the best of [his] knowledge, [he] never received a copy of KLC's Employee Handbook" (Benitez Decl. re: P.O. ¶ 13), Defendants have presented evidence that Mr. Benitez received two emails dated November 19, 2007 and February 23, 2009, both of which included the KLC Handbook as an attachment. (2nd Keegan Decl. Exs. 1 & 2.) Mr. Benitez does not ever expressly deny receiving these emails. In light of Defendants' undisputed evidence of Mr. Benitez's receipt of these two emails, Mr. Benitez's best recollections that he did not receive the handbook must yield. Based on the evidence presented, the court must conclude that Mr. Benitez did in fact receive copies of the KLC Employee Handbook on more than one occasion.

[35] In any event, Mr. Benitez was a vice-president of KCDL and a member of KCDL's executive committee. (Knowles Decl. Ex. B (Benitez Dep.) at 150:24–151:1, 151:2–19; Ex. A (Brown Dep.) at 262:8–263:12.) As a senior level manager, Mr. Benitez was "expected to know the contents of company policies so [he] could properly manage and supervise employees." (2nd Keegan Decl. ¶ 4.) Accordingly, Mr. Benitez is fairly charged with constructive knowledge of the company's policies concerning electronic communications. *See, e.g.*, *Scott v. Beth Israel Med. Center, Inc.*, 17 Misc.3d 934, 847 N.Y.S.2d 436, 441 (Sup.Ct.2007) ("[Former employee's] effort to maintain that he was unaware of [former employer's] email policy barring personal use is rejected. As an administrator, [former employee] had constructive knowledge of the policy.").

KLC's handbook contains an Electronic Communications policy which clearly states that "[e]lectronic communications are not private." (1st Keegan Decl. ¶ 3, Ex. 2.) The policy also states that "[a]ll resources used for electronic communications are KLC property" and "should generally be used only for KLC business." (*Id.*) Finally, the policy states that KLC "reserves the right to access, search, inspect, monitor, record, and disclose any file or stored communication ... at any time and for any reason." (*Id.*)

[36] Washington law protects only confidential communications between an attorney and a client. *Morgan*, 213 P.3d at 601 ("To qualify for attorney-client privilege, a communication must be made in confidence."***1108**) For the privilege to apply, the client must have a reasonable expectation that the communications are confidential and will be kept confidential. *In re Siegfried*, 42 Wash.App. 21, 708 P.2d 402, 404–05 (Wash.Ct.App.1985) (analyzing psychologist-patient communications privilege which "are privileged to the same extent, and are subject to

the same conditions, as are confidential communications between attorney and client"). If a client is informed that there may be disclosure to a third-party, there is no reasonable expectation of confidentiality and the privilege never attaches. *See Hertog v. City of Seattle*, 138 Wash.2d 265, 979 P.2d 400, 411 (1999) (analyzing psychologist-patient communications); *see also State v. Side*, 105 Wash.App. 787, 21 P.3d 321, 324–25 (Wash.Ct.App.2001) (analyzing psychologist-patient communications, the court held that "[a] patient who is warned that communications may not be kept confidential has no reasonable expectation of confidentiality and any privilege is waived.").

[37] Based on the company policy described above, Mr. Benitez could not have had a reasonable expectation of confidentiality with regard to communications or other materials that he created or received on his KCDL laptop following the acquisition of Aventa and that were saved or stored on his KCDL laptop or the Defendants' servers. The laptop itself was not his property, and the company reserved the right to access and disclose any file or stored communication at any time. Thus, Mr. Benitez cannot meet his burden of proving that any expectation of confidentiality he might have entertained was reasonable.[FN16] Accordingly, the court finds that the attorney-client privilege never attached with regard to emails or communications that Mr. Benitez created and sent or that he received after the Aventa acquisition, which were stored on his KCDL laptop or the Defendants' servers.[FN17]

FN16. Mr. Benitez argues that Defendants must show that he received the company policy before transferring the emails to his laptop. First, as discussed above, the burden of establishing the existence of the attorney-client privilege, including lack of waiver, is on Plaintiffs. *See Dietz*, 935 P.2d at 618–19; *see also Perrow*, 231 P.3d at 856. Second, Defendants did provide evidence of that the Employee Handbook was sent to all new Aventa employees upon commencement of employment. (*See* 1st Keegan Decl. ¶ 6, Ex. 4.) Even if Mr. Benitez received the policy after he transferred his privileged email to his laptop, upon receiving the policy and learning that his laptop was not confidential, he should have promptly taken steps to protect the privileged material. Instead, he did nothing for years and did not attempt to assert the privilege until his employment with KCDL had ended. Based on this inaction, the court finds that it would be no defense to waiver even if Mr. Benitez had not receive the policy until after he had transferred confidential communications to his laptop.

FN17. Although the court previously held that Mr. Axtman waived any applicable privilege when he unconditionally relinquished his laptop to KCDL following his separation from the company, the court's analysis here concerning Mr. Benitez would also apply to Mr. Axtman as additional grounds for granting Defendants' motion for a protective order.

[38] In addition, to the extent that Mr. Benitez saved attorney-client privileged communications or documents created before the Aventa acquisition onto his KCDL laptop, he waived any privilege that may have previously attached to these materials.[FN18] Although Washington courts have not yet addressed this issue specifically, most state and federal courts evaluating ***1109** whether an employee has waived the attorney-client privileged status of personal communications transmitted, stored, or saved onto a company computer or laptop, have applied the four-factor test initially set forth in *In re Asia Global*, 322 B.R. 247, 257 (Bankr.S.D.N.Y.2005). *See In re Reserve Fund Sec. & Derivative Litig.*, 275 F.R.D. 154, 159–60 (S.D.N.Y.2011) (describing *Asia Global* as "widely adopted" and listing myriad cases). The *Asia Global* factors are: (1) does the company maintain a policy

banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or email, (3) do third parties have a right of access to the computer or emails, and (4) did the corporation notify the employee, or was the employee aware, of the policy. *Asia Global,* 322 B.R. at 257.

> FN18. Although the court has already found that privilege did not attach to files or communications that Mr. Benitez created or received on KCDL laptop following the acquisition of Aventa, this waiver analysis would also apply to these files or communications as an additional ground for granting Defendants' motion.

With regard to the first factor, the company's policy states that "resources used for electronic communications ... should generally be used only for KLC business." (1st Keegan Decl. ¶ 3, Ex. 2 at 21.) Although the company policy does not place an outright ban on any personal use, personal use is discouraged. Further, the policy expressly warns employees that electronic communications are not private. Consequently, it would not be reasonable for an employee to believe that such communications stored on company hardware would be confidential. With regard to the second factor, not only does the company policy expressly state that any stored communication or file can be monitored, recorded and disclosed, the company does in fact conduct such monitoring. (1st Keegan Decl. ¶ 5.) Although there is no evidence that KCDL ever specifically monitored Mr. Benitez's computer during his employment, courts have found that a policy permitting such monitoring meets this factor. *See, e.g., Scott,* 847 N.Y.S.2d at 442. For the third factor, the policy expressly allows the company to access information and to disclose it. Finally, the court has previously addressed the fourth factor and found that Mr. Benitez had both actual and constructive notice of the company's policies. Accordingly, the *Asia Global* factors have been met, and the court concludes that Mr. Benitez waived any privilege that may have attached to the communications or files at issue here when he saved or stored them on his KCDL laptop computer.[FN19]

> FN19. Although the court previously found that Mr. Axtman waived any privilege when he unconditionally relinquished his laptop to KCDL, the court's waiver analysis with regard to Mr. Benitez under the *Asia Global* factors would be equally applicable to Mr. Axtman, and provides additional grounds for finding waiver of the privilege in his case.

Some courts have found an exception maintaining an employee's expectation of privacy at least with regard to attorney-client communications accessed on personal, password-protected, web-based email—even if the employee accesses the web-based account using the company's computer system and the company maintains a policy against such use. *See, e.g., Stengart v. Loving Care Agency, Inc.,* 201 N.J. 300, 990 A.2d 650, 665 (2010) ("Because of the important public policy concerns underlying the attorney-client privilege, even ... a policy that banned all personal computer use and provided unambiguous notice that an employer could retrieve and read an employee's attorney-client communications, if accessed on a personal, password-protected e-mail account using the company's computer system—would not be enforceable."). In particular, Mr. Benitez and Mr. Axtman rely upon *Sims v. Lakeside School,* No. C06–1412RSM, 2007 WL 2745367 (W.D.Wash. Sept. 20, 2007). In *Sims,* the court found that, based on the school/employer's policy, the employee had no reasonable expectation of privacy in the ***1110** contents of his laptop, and that his absence of privacy rights also extended to the emails he sent and received on the school's accounts. *Id.* at *1. The court, nevertheless, held to the contrary with regard to web-based emails sent and received by the plaintiff on his school laptop. *Id.* at *2. The *Sims* court does not provide a rationale for its distinction other than general public policy grounds and the importance of the attor-

ney-client privilege. *Id.*

Although this court is in accord with regard to the value of the attorney-client privilege, it does believe that *Sims* is applicable here. The *Sims* court does not specifically address choice of law, but it appears to have based its analysis on federal law. *See id.* Here, the court's analysis must be grounded in and consistent with its view of Washington law. Washington has a policy of "strictly limiting the attorney-client privilege to its purpose." *Sitterson v. Evergreen Sch. Dist. No. 114*, 147 Wash.App. 576, 196 P.3d 735, 741 (Wash.Ct.App.2008). In *Sitterson*, the court was considering whether to adopt an approach to inadvertent production of the attorney-client communications which (1) never waived the privilege, or (2) which considered the circumstances of the case. *Id.* at 740–42. The *Sitterson* court found that a non-waiver rule "is inconsistent with Washington's policy." *Id.* at 741. The court stated:

> The privilege is so limited because it sometimes results in the exclusion of relevant and material evidence, contrary to the philosophy that justice requires the fullest disclosure of the facts.... Consequently, employing the attorney-client privilege to prohibit testimony must be balanced against the benefits to the administration of justice stemming from the general duty to give what testimony one is capable of giving.... These considerations weigh toward taking a broader view of waiver than the [defendant] proposes.

Id. (citations and quotations omitted). As a result, the court rejected a rule in which inadvertent disclosure could never waive the attorney-client privilege. Instead, the court adopted a "balanced approach," in which the court considered a variety factors surrounding the inadvertent disclosure in determining whether waiver had occurred. *Id.* at 741–42.

Following *Sitterson*, this court believes that Washington would also take a broader view of the waiver issue here, and adopt a balanced approach and not a non-waiver rule concerning web-based personal email accounts that are accessed through an employee's company computer or laptop. Accordingly, the court does not believe that decisions such as *Stengart* or *Sims*, which adopt a no-waiver rule concerning web-based personal email accounts accessed through an employee's company-issued computer or laptop, are applicable in Washington. Applying the balanced-approach outlined in *Asia Global*, the court can find no reason to distinguish between emails that were sent from or received on the company's email system and emails that were accessed through the company's laptop on Mr. Benitez's or Mr. Axtman's web-based email accounts. The company's policy here was broad. It applied to "[a]ll resources used for electronic communications" and stated that these resources were KLC property. (1st Keegan Decl. ¶ 3, Ex. 2.) Further, the policy reserved the company's right "to access, search, ... or disclose *any file or stored communication.*" (*Id.* (italics added).) To the extent that Mr. Benitez's or Mr. Axtman's emails from their web-based personal email accounts are stored on their KCDL laptops or the Defendants' servers, those emails would be encompassed by the policy. Accordingly, based on the *Asia Global* factors analyzed above, any privilege that once may have applied to these communications is waived.

*1111 IV. CONCLUSION

Based on the forgoing, the court GRANTS in part and DENIES in part Defendants' motion for summary judgment (Dkt. # 81), DENIES Plaintiffs' motion to dismiss the counterclaims (Dkt. # 58), and GRANTS Defendants' motion for a protective order (Dkt. # 61).

W.D.Wash.,2011.
Aventa Learning, Inc. v. K12, Inc.
830 F.Supp.2d 1083, Blue Sky L. Rep. P 74,956

END OF DOCUMENT

830 F.Supp.2d 1083, Blue Sky L. Rep. P 74,956
(Cite as: 830 F.Supp.2d 1083)

Not Reported in F.Supp.2d, 2010 WL 960348 (N.D.Ill.)
(Cite as: 2010 WL 960348 (N.D.Ill.))

H

Only the Westlaw citation is currently available.

United States District Court,
N.D. Illinois,
Eastern Division.
MOTOROLA, INC., Plaintiff,
v.
LEMKO CORP., Shaowei Pan, Hanjuan Jin, Xiaohua Wu, Xuefeng Bai, Xiaohong Sheng, Nicholas Labun, Bohdan Pyskir, Hechun Cai, Jinzhong Zhang, Angel Favila, Ankur Saxena, Raymond Howell, Faye Vorick, and Nicholas Desai, Defendants.

No. 08 C 5427.
March 15, 2010.

West KeySummary**Civil Rights 78 1395(8)**

78 Civil Rights
78III Federal Remedies in General
78k1392 Pleading
78k1395 Particular Causes of Action
78k1395(8) k. Employment Practices. Most Cited Cases

Chinese female employee alleged sufficient facts to save her discrimination claim under § 1981 from dismissal. Employee was terminated due to her suspected role in an alleged trade secret theft. In her claim, employee alleged that she was treated contrary to company policy when she was terminated for an offense that only warranted a written warning for a first offense. Employee presented evidence that only Chinese nationals were targeted in the investigation and that company policy had been followed when applied to white employees born in the United States. 42 U.S.C.A. § 1981(a).

Robert Mark Halligan, Deanna R. Swits, Jodi Rosen Wine, Michael Christian Hallerud, Nixon Peabody LLP, Chicago, IL, for Plaintiff.

Michael Dean Karpeles, Barry Ryan Horwitz, Charles B. Leuin, Jonathan Hale Claydon, Richard Daniel Harris, Greenberg Traurig, LLP., Telly Stefaneas, Telly Stefaneas, Esq., William J. Leonard, Wang, Leonard & Condon, Gregory Adam Adamski, Adamski & Conti, Chicago, IL, for Defendants.

Raymond Howell, Mundelein, IL, pro se.

MEMORANDUM OPINION AND ORDER

MATTHEW F. KENNELLY, District Judge.

***1** Plaintiff Motorola, Inc. has moved to dismiss the counterclaim of defendant Shaowei Pan pursuant to Federal Rule of Civil Procedure 12(b)(6) and has moved for judgment on the pleadings pursuant to Rule 12(c) on the counterclaim of Xiaohong Sheng. For the reasons stated below, the Court grants the motions in part and denies them in part.

Background

Motorola has sued Pan, Sheng, and several others under the Computer Fraud and Abuse Act and for misappropriation of trade secrets and other claims. Pan worked for Motorola from 1994 through early April 2004 and is now the chief technology officer of defendant Lemko Corp. He is also the spouse of defendant Xiaohua Wu, who worked for Motorola as an engineer from 1995 through December 2007. Motorola alleges that in 2005–2007, Wu obtained confidential and proprietary Motorola information and transferred it to Lemko.

Sheng worked for Motorola as a software engineer from November 2006 through July 2008. Motorola alleges that while working for the company, Sheng secretly continued to work for Lemko, where

she had been employed. According to Motorola, Sheng (among other things) improperly downloaded confidential and proprietary Motorola information without its consent and used a Motorola-provided computer to perform work for Lemko.

1. Sheng's counterclaim

Sheng has filed a four-count counterclaim against Motorola. Count 1 is a claim for abuse of process. Sheng alleges that she did not possess or use any Motorola trade secret and that Motorola had no reason to think she did when it sued her. She also alleges that Motorola has misrepresented the communications that it alleges constituted improper transmission of confidential or proprietary information. According to Sheng, "Motorola brought this lawsuit to coerce Sheng to assist in civil and criminal claims against [defendant Hanjuan] Jin, and/or to use [Sheng] as an example to intimidate its past, present, and future employees who may assert their rights against it or be 'more loyal to their friends' than to Motorola." Sheng Counterclaim ¶ 53.

In Count 2, Sheng alleges that Motorola discriminated against her based on her Chinese ethnicity. She alleges that Motorola investigated only Chinese nationals and Asians when investigating Jin's alleged trade secret theft and did not file suit against any white person or anyone born in the United States relating to that theft but rather sued only Chinese nationals and Asians. She also alleges that Motorola terminated her for an infraction that, under Motorola's standard policies, subjected a person only to a written warning for a first offense. She alleges that Motorola acted contrary to these policies because of her race and alienage and that it follows its policies when applying them to white persons born in the United States. Sheng alleges that Motorola would not have terminated her employment or filed suit against her had she not been a Chinese national or Asian.

In Count 3, Sheng alleges that Motorola provided her with a computer and understood she would use it to work from home. She says that Motorola allowed its employees to occasionally check their personal e-mail from Motorola-issued computers and that she did so occasionally. She alleges that she took steps to secure her personal e-mail account and that she had a reasonable expectation that the contents of that account were private. Despite this, Sheng alleges, Motorola intentionally viewed the contents of her private, web-based e-mail account.

***2** Count 4 is a claim under the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, based on the same allegations that underlie Count 3. Sheng alleges that Motorola, without authorization, "intentionally accessed a facility through which an electronic communication service is provided," Sheng Counterclaim ¶ 91, to obtain access to electronic communications in electronic storage.

2. Pan's counterclaim

Pan has filed a six-count counterclaim seeking a declaratory judgment on various issues (Counts 1, 3, and 5) and damages for unjust enrichment (Counts 2, 4, and 6). Pan alleges that while at Lemko, he actually invented or co-invented a number of the inventions that Motorola claims are its trade secrets that he misappropriated. He contends that Motorola took advantage of these technologies as if it owned them exclusively.

Pan alleges that while at Motorola, he contributed to or created at least sixty patented inventions assigned to Motorola. He says that when, after his departure from Motorola, his wife Wu's team began to work on "cellular location technology," he "began unofficially advising and collaborating with the team, repeatedly giving them the benefit of his knowledge and experience." Pan Counterclaim ¶ 2. During this period of advice and collaborating, Pan alleges, Wu submitted several inventions to Motorola for consideration. Motorola filed for patents on some and maintained others as trade secrets and has used a number of them, including inventions referred to as the hybrid location

determination trade secret, the AP geometry location determination trade secret, and the tracking invention. (These are some of the same matters that, according to Motorola, Pan misappropriated or assisted in misappropriating from Motorola.) Pan alleges that he received no compensation for these inventions and that Motorola has made millions of dollars from them. Pan seeks a declaratory judgment that he is an owner or co-owner of all three inventions and damages consisting of the market value of one of them (on which Motorola filed but abandoned a patent application) and Motorola's profits from the others.

Discussion

When considering a motion to dismiss under Rule 12(b)(6), the Court accepts the facts stated in the complaint as true and draws reasonable inferences in favor of the plaintiff. *Hallinan v. Fraternal Order of Police of Chicago Lodge No. 7*, 570 F.3d 811, 820 (7th Cir.2009). To survive the motion, the complaint must include enough facts to state a claim for relief that is plausible on its face. *Ashcroft v. Iqbal*, —— U.S. ——, ——, 129 S.Ct. 1937, 1950, 173 L.Ed.2d 868 (2009). A claim is plausible on its face "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* at 1949. Though a complaint need not include "detailed factual allegations, a plaintiff's obligation to provide the grounds of his entitlement to relief requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007) (internal citations omitted). A motion for judgment on the pleadings under Rule 12(c) is considered under the same standard that applies to a Rule 12(b)(6) motion. *Buchanan–Moore v. County of Milwaukee*, 570 F.3d 824, 827 (7th Cir.2009).

1. Sheng's counterclaim

a. Abuse of process claim

***3** To succeed on her claim for abuse of process, Sheng must prove an ulterior motive or purpose by Motorola in the use of regular court process and some act in the legal process not proper in the regular prosecution of the proceedings. *See, e.g., Commerce Bank, N.A. v. Plotkin*, 255 Ill.App.3d 870, 872, 637 N.E.2d 746, 748 (1994); *Sutton v. Hofeld*, 118 Ill.App.3d 65, 69, 73 Ill.Dec. 584, 454 N.E.2d 681, 683 (1983). But "the mere filing of a lawsuit even with a malicious motive does not constitute an abuse of process." *Sutton*, 118 Ill.App.3d at 70, 73 Ill.Dec. 584, 454 N.E.2d at 684. Illinois courts "have generally taken a very restrictive view of the tort of abuse of process. The word 'process' has been given its literal meaning." *Commerce Bank*, 255 Ill.App.3d at 872, 194 Ill.Dec. 409, 627 N.E.2d at 748.

Count 1 fails to state an abuse of process claim. Sheng's allegation that Motorola filed suit to intimidate her is insufficient without more. Specifically, she has not alleged any act by Motorola in the use of court process that was not proper in the regular prosecution of the case. *See, e.g., Sanchez & Daniels v. Koresko & Assocs.*, No. 04 C 5183, 2006 WL 3235604, at *6 (N.D.Ill. Nov. 8, 2006) (citing cases).

b. Discrimination claim

In her response to Motorola's motion to dismiss, Sheng has clarified that Count 2 is a claim under 42 U.S.C. § 1981(a), which provides that "[a]ll persons with in the jurisdiction of the United States shall have the same right ... to make and enforce contracts, to sue, be parties, give evidence, and to the full and equal benefit of all laws and proceedings for the security of persons and property as is enjoyed by white citizens ...." The term "make and enforce contracts" is defined to include "the making, performance, modification, and termination of contracts, and the enjoyment of all benefits, privileges, terms, and conditions of the contractual relationship." *Id.* § 1981(b).

It is questionable whether Motorola's allegedly improper referral of Sheng to federal law enforcement authorities and its investigation and filing of suit against her qualify as actions that adversely impact Sheng's rights relating to the making and enforcement of contracts. The termination of her employment, however, is the type of conduct that may be actionable under section 1981(a).

Section 1981 encompasses only claims of discrimination based on race, not national origin. But the Supreme Court has defined race "broadly to include identifiable classes of persons who are subjected to intentional discrimination solely because of their ancestry or ethnic characteristics." *Ptasznik v. St. Joseph Hosp.* ., 464 F.3d 691, 695 n. 4 (7th Cir.2006) (citing *St. Francis Coll. v. Al–Khazraji*, 481 U.S. 604, 609, 107 S.Ct. 2022, 95 L.Ed.2d 582(1987)). Sheng's allegation that Motorola terminated her employment because of her Chinese ethnicity is sufficient to bring her claim within section 1981(a).

Motorola alleges that Sheng has not alleged sufficient facts to state a discrimination claim. The Court disagrees. Sheng is not required to prove her case in her complaint, even in the post-*Twombly* and *Iqbal* environment: the Federal Rules still follow a notice-pleading regime, and they do not "impose a probability requirement on plaintiffs." *Brooks v. Ross*, 578 F.3d 574, 581 (7th Cir.2009). Sheng alleges that Motorola acted contrary to its usual policies and treated her alleged infraction more severely than it treated similar infractions by white persons. The Court must take this allegation as true for present purposes. This, plus the other allegations in Count 2, are sufficient to save her claim from dismissal.

c. Intrusion upon seclusion claim

***4** To sustain a claim of intrusion upon seclusion under Illinois law—a form of invasion of privacy claim—Sheng must show that Motorola committed an unauthorized intrusion or prying into her seclusion that would be highly offensive or objectionable to a reasonable person, intruded into a private matter, and caused the plaintiff anguish and suffering. *See, e.g.*, *Busse v. Motorola, Inc.*, 351 Ill.App.3d 67, 71, 286 Ill.Dec. 320, 813 N.E.2d 1013, 1017 (2004). As indicated earlier, Sheng alleges that Motorola looked at the contents of her private e-mail account, which Sheng had accessed via a Motorola-provided computer. *See* Sheng Counterclaim ¶¶ 77–87.

Sheng's claim is insufficient because she has not alleged that Motorola's intrusion was unauthorized. The Court does not reach this conclusion based on Motorola's reference to a "usage notice" that it contends was posted on Sheng's company-issued computer in which it reserved the right to inspect any electronic communication transmitted via the computer or via Motorola's network. *See* Motorola Mem. at 11 n. 2. That is a reference to a document outside the pleadings, which the Court cannot properly consider in the present procedural context. Rather, the Court rules as it does because Sheng's counterclaim contains no allegation that Motorola's alleged intrusion was unauthorized.[FN1] For this reason, the Court need not consider Motorola's other arguments in support of dismissal.

> FN1. If Sheng attempts to replead this claim in a sufficient manner via an amended counterclaim, she and her counsel should of course be aware that Federal Rule of Civil Procedure 11(b)(3) makes it improper to make a factual allegation that does not have evidentiary support or is unlikely to have such support after a reasonable opportunity for discovery. If Motorola is correct about the usage notice, Sheng would be well advised in any amended counterclaim to acknowledge its existence and then allege (if she has a viable basis to do so) why it does not apply or otherwise bar her claim.

d. Stored Communications Act claim

The Stored Communications Act permits a person

aggrieved by a knowing or intentional violation of the Act to recover damages from the violator. 18 U.S.C. § 2707(a). Sheng does not identify the particular provision of the Act she contends Motorola violated. But based upon her allegations, it appears that she alleges that Motorola violated 18 U.S.C. § 2701(a), which prohibits a person from "intentionally access[ing] without authorization a facility through which an electronic communication service is provided" and from "intentionally exceed[ing] an authorization to access that facility ."

Sheng's Stored Communications Act claim fails for the same reason that her intrusion upon seclusion claim was deficient. Specifically, Sheng has not alleged that Motorola's access was without authorization. The Court thus need not deal with whether her claim otherwise meets the requirements under the Act.

2. Pan's counterclaim

a. Unjust enrichment claims

"The doctrine of unjust enrichment underlies a number of legal and equitable actions and remedies, including the equitable remedy of constructive trust and the legal actions of assumpsit and restitution or quasi-contract. To state a cause of action based on a theory of unjust enrichment, a plaintiff must allege that the defendant has unjustly retained a benefit to the plaintiff's detriment, and that defendant's retention of the benefit violates the fundamental principles of justice, equity, and good conscience." *HPI Health Care Servs., Inc. v. Mt. Vernon Hosp., Inc.*, 131 Ill.2d 145, 154, 137 Ill.Dec. 19, 545 N.E.2d 672, 676 (1989)

***5** A claim for unjust enrichment may be asserted in the present context when one party performs a service for the benefit of another, the other party accepts the benefit, and the surrounding circumstances indicate that the service was not intended to be gratuitous. *See, e.g., Midwest Emerg. Assocs.-Elgin Ltd. v. Harmony Health Plan of Ill., Inc.*, 382 Ill.App.3d 973, 982, 321 Ill.Dec. 175, 888 N.E.2d 694, 701 (2008) Generally speaking, a person who "perform[s] services altruistically or gratuitously, with some end other than payment in mind," cannot recover for unjust enrichment. *Midcoast Aviation, Inc. v. General Electric Credit Corp.*, 907 F.2d 732, 740 (7th Cir.1990).

Pan points out that statements by courts along these lines generally have been made in the context of *quantum meruit* claims and that he is not making such a claim.[FN2] Whether or not that is so, but Pan still has to show—or at this point, to allege plausibly—that Motorola was *unjustly* enriched. With that in mind, the statements by courts in *quantum meruit*-based unjust enrichment cases along the lines that "with no expectation of payment for services rendered, a party can hardly claim that another has been *unjustly* enriched," *id.*, apply equally in the present context. *Id.* (emphasis in original). *See also, e.g., Cosgrove v. Bartolotta*, 150 F.3d 729, 734 (7th Cir.1998) (Wisconsin law; to recover for unjust enrichment, benefactor must reasonably believe he will be paid, "that is, when the benefit is not rendered gratuitously ... or donatively, as by an altruist or friend or relative").

FN2. Pan cites no authority, however, sustaining an unjust enrichment claim in the present context.

Sheng does not allege that he was expecting a benefit; rather, he alleges that he was helping out his spouse. Illinois law applies a presumption that a person who furnishes services to a family member does so gratuitously, *see, e.g., In re Templeton*, 339 Ill.App.3d 310, 314, 273 Ill.Dec. 833, 789 N.E.2d 1265, 1268 (2003), and Pan alleges nothing that hints he can rebut that presumption. For this reason, he has failed to state a claim for unjust enrichment.

b. Declaratory judgment claims

The Court denies Motorola's motion to dismiss with regard to Pan's declaratory judgment claims. Motorola relies largely on its own complaint against Pan as well as other documents that are not part of Pan's counterclaim. The Court cannot consider these materials in the present procedural posture of the case.

Conclusion

For the reasons stated in this decision, the Court grants Motorola's motions to dismiss and for judgment of the pleadings [311 & 315] in part and denies them in part. Counts 1, 3, and 4 of Sheng's counterclaim are dismissed, as are Counts 2, 4, and 6 of Pan's counterclaim. Motorola's motions are otherwise denied. Motorola is directed to answer the remaining claims on or before March 29, 2010.

N.D.Ill.,2010.
Motorola, Inc. v. Lemko Corp.
Not Reported in F.Supp.2d, 2010 WL 960348 (N.D.Ill.)

END OF DOCUMENT

560 U.S. 746, 130 S.Ct. 2619, 93 Empl. Prac. Dec. P 43,907, 177 L.Ed.2d 216, 78 USLW 4591, 159 Lab.Cas. P 61,011, 30 IER Cases 1345, 10 Cal. Daily Op. Serv. 7565, 2010 Daily Journal D.A.R. 9072, 22 Fla. L. Weekly Fed. S 470

(Cite as: 560 U.S. 746, 130 S.Ct. 2619)

Supreme Court of the United States

CITY OF ONTARIO, CALIFORNIA, et al., Petitioners,

v.

Jeff QUON et al.

No. 08–1332.

Argued April 19, 2010.

Decided June 17, 2010.

Background: City police officer brought § 1983 action against city, police department, police chief, alleging that police department's review of officer's text messages violated Fourth Amendment, and asserted claim against wireless communications provider under Stored Communications Act (SCA). The United States District Court for the Central District of California, Stephen G. Larson, J., 445 F.Supp.2d 1116, granted summary judgment for wireless provider on SCA claim, and, following jury determination as to chief's intent in ordering review of text messages, entered judgment in favor of remaining defendants on Fourth Amendment and related state-law claims. Officer appealed. The Ninth Circuit Court of Appeals, Wardlaw, Circuit Judge, 529 F.3d 892, affirmed in part and reversed in part, holding that officer had reasonable expectation of privacy in text messages but that search was not reasonable. City's petition for certiorari was granted.

Holding: The Supreme Court, Justice Kennedy, held that city's review of officer's text messages was reasonable, and thus did not violate Fourth Amendment.

Reversed and remanded.

Justice Stevens filed concurring opinion.

Justice Scalia filed opinion concurring in part and concurring in judgment.

West Headnotes

[1] Searches and Seizures 349 23

349 Searches and Seizures

349I In General

349k23 k. Fourth Amendment and reasonableness in general. Most Cited Cases

The Fourth Amendment's protection extends beyond the sphere of criminal investigations. U.S.C.A. Const.Amend. 4.

[2] Searches and Seizures 349 23

349 Searches and Seizures

349I In General

349k23 k. Fourth Amendment and reasonableness in general. Most Cited Cases

The Fourth Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government, without regard to whether the government actor is investigating crime or performing another function. U.S.C.A. Const.Amend. 4.

[3] Searches and Seizures 349 31.1

349 Searches and Seizures

349I In General

349k31 Persons Subject to Limitations; Governmental Involvement

349k31.1 k. In general. Most Cited Cases

The Fourth Amendment applies when the Government acts in its capacity as an employer. U.S.C.A. Const.Amend. 4.

[4] Searches and Seizures 349 31.1

349 Searches and Seizures
349I In General
349k31 Persons Subject to Limitations; Governmental Involvement
349k31.1 k. In general. Most Cited Cases

Searches and Seizures 349 36.1

349 Searches and Seizures
349I In General
349k36 Circumstances Affecting Validity of Warrantless Search, in General
349k36.1 k. In general. Most Cited Cases

Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer, and special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable for government employers. U.S.C.A. Const.Amend. 4.

[5] Searches and Seizures 349 36.1

349 Searches and Seizures
349I In General
349k36 Circumstances Affecting Validity of Warrantless Search, in General
349k36.1 k. In general. Most Cited Cases

Assuming that the appropriate test for analyzing Fourth Amendment claims against government employers is that of the *O'Connor v. Ortega* plurality, the first step of such an analysis is that, because some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable, a court must consider the operational realities of the workplace in order to determine whether an employee's Fourth Amendment rights are implicated; on this view, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis. U.S.C.A. Const.Amend. 4.

[6] Searches and Seizures 349 36.1

349 Searches and Seizures
349I In General
349k36 Circumstances Affecting Validity of Warrantless Search, in General
349k36.1 k. In general. Most Cited Cases

Assuming that the appropriate test for analyzing Fourth Amendment claims against government employers is that of the *O'Connor v. Ortega* plurality, the second step of such an analysis is that, where an employee has a legitimate privacy expectation, an employer's intrusion on that expectation for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances. U.S.C.A. Const.Amend. 4.

[7] Searches and Seizures 349 36.1

349 Searches and Seizures
349I In General
349k36 Circumstances Affecting Validity of Warrantless Search, in General
349k36.1 k. In general. Most Cited Cases

Assuming that the appropriate test for analyzing Fourth Amendment claims against government employers is that of Justice Scalia's concurrence in the judgment in *O'Connor v. Ortega*, it is appropriate to dispense with an inquiry into operational realities and

to conclude that the offices of government employees are covered by Fourth Amendment protections as a general matter; however, government searches to retrieve work-related materials or to investigate violations of workplace rules, which are searches of the sort that are regarded as reasonable and normal in the private-employer context, do not violate the Fourth Amendment. U.S.C.A. Const.Amend. 4.

[8] Searches and Seizures 349 36.1

349 Searches and Seizures
349I In General
349k36 Circumstances Affecting Validity of Warrantless Search, in General
349k36.1 k. In general. Most Cited Cases

Telecommunications 372 1436

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General
372k1435 Acts Constituting Interception or Disclosure
372k1436 k. In general. Most Cited Cases

The Supreme Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer, and the judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. U.S.C.A. Const.Amend. 4.

[9] Searches and Seizures 349 24

349 Searches and Seizures
349I In General
349k24 k. Necessity of and preference for warrant, and exceptions in general. Most Cited Cases

Although as a general matter, warrantless searches are per se unreasonable under the Fourth Amendment, there are a few specifically established and well-delineated exceptions to that general rule, and the special needs of the workplace justify one such exception. U.S.C.A. Const.Amend. 4.

[10] Searches and Seizures 349 23

349 Searches and Seizures
349I In General
349k23 k. Fourth Amendment and reasonableness in general. Most Cited Cases

It is not the case that only the least intrusive search practicable can be reasonable under the Fourth Amendment. U.S.C.A. Const.Amend. 4.

[11] Telecommunications 372 1438

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General
372k1435 Acts Constituting Interception or Disclosure
372k1438 k. Wireless or mobile communications. Most Cited Cases

Assuming that police officer had reasonable expectation of privacy in text messages sent on pager provided to him by city, that city's review of transcript of officer's text messages constituted “search,” and that principles applicable to government employer's search of employee's physical office apply with at least the same force when employer intrudes on employee's privacy in the electronic sphere, city's review of officer's text messages was reasonable, and thus did

not violate Fourth Amendment, in that search was motivated by legitimate work-related purpose of determining whether character limit on city's contract with wireless communications provider was sufficient to meet city's needs, and search was not excessively intrusive in light of that justification. U.S.C.A. Const.Amend. 4.

*****2621 *746** *Syllabus* [FN*]

FN* The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States v. Detroit Timber & Lumber Co.*, 200 U.S. 321, 337, 26 S.Ct. 282, 50 L.Ed. 499.

Petitioner Ontario (hereinafter City) acquired alphanumeric pagers able to send and receive text messages. Its contract with its service provider, Arch Wireless, provided for a monthly limit on the number of characters each pager could send or receive, and specified that usage exceeding that number would result in an additional fee. The City issued the pagers to respondent Quon and other officers in its police department (OPD), also a petitioner here. When Quon and others exceeded their monthly character limits for several months running, petitioner Scharf, OPD's chief, sought to determine whether the ****2622** existing limit was too low, *i.e.*, whether the officers had to pay fees for sending work-related messages or, conversely, whether the overages were for personal messages. After Arch Wireless provided transcripts of Quon's and another employee's August and September 2002 text messages, it was discovered that many of Quon's messages were not work related, and some were sexually explicit. Scharf referred the matter to OPD's internal affairs division. The investigating officer used Quon's work schedule to redact from his transcript any messages he sent while off duty, but the transcript showed that few of his on-duty messages related to police business. Quon was disciplined for violating OPD rules.

He and the other respondents—each of whom had exchanged text messages with Quon during August and September—filed this suit, alleging, *inter alia*, that petitioners violated their Fourth Amendment rights and the federal Stored Communications Act (SCA) by obtaining and reviewing the transcript of Quon's pager messages, and that Arch Wireless violated the SCA by giving the City the transcript. The District Court denied respondents summary judgment on the constitutional claims, relying on the plurality opinion in *O'Connor v. Ortega*, 480 U.S. 709, 107 S.Ct. 1492, 94 L.Ed.2d 714, to determine that Quon had a reasonable expectation of privacy in the content of his messages. Whether the audit was nonetheless reasonable, the court concluded, turned on whether Scharf used it for the improper purpose of determining if Quon was using his pager to waste time, or for the legitimate purpose of determining the efficacy of existing character limits to ensure that officers were not paying hidden ***747** work-related costs. After the jury concluded that Scharf's intent was legitimate, the court granted petitioners summary judgment on the ground they did not violate the Fourth Amendment. The Ninth Circuit reversed. Although it agreed that Quon had a reasonable expectation of privacy in his text messages, the appeals court concluded that the search was not reasonable even though it was conducted on a legitimate, work-related rationale. The opinion pointed to a host of means less intrusive than the audit that Scharf could have used. The court further concluded that Arch Wireless had violated the SCA by giving the City the transcript.

Held: Because the search of Quon's text messages was reasonable, petitioners did not violate respondents' Fourth Amendment rights, and the Ninth Circuit erred by concluding otherwise. Pp. 2627 – 2633.

(a) The Amendment guarantees a person's privacy, dignity, and security against arbitrary and inva-

sive governmental acts, without regard to whether the government actor is investigating crime or performing another function. *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602, 613–614, 109 S.Ct. 1402, 103 L.Ed.2d 639. It applies as well when the government acts in its capacity as an employer. *Treasury Employees v. Von Raab*, 489 U.S. 656, 665, 109 S.Ct. 1384, 103 L.Ed.2d 685. The Members of the *O'Connor* Court disagreed on the proper analytical framework for Fourth Amendment claims against government employers. A four-Justice plurality concluded that the correct analysis has two steps. First, because "some [government] offices may be so open ... that no expectation of privacy is reasonable," a court must consider "[t]he operational realities of the workplace" to determine if an employee's constitutional rights are implicated. 480 U.S., at 718, 107 S.Ct. 1492. Second, where an employee has a legitimate privacy expectation, an employer's intrusion on that expectation "for noninvestigatory, work-related purposes, as well as for investigations of work-****2623** related misconduct, should be judged by the standard of reasonableness under all the circumstances." *Id.*, at 725–726, 107 S.Ct. 1492. Justice SCALIA, concurring in the judgment, would have dispensed with the "operational realities" inquiry and concluded "that the offices of government employees ... are [generally] covered by Fourth Amendment protections," *id.*, at 731, 107 S.Ct. 1492, but he would also have held "that government searches to retrieve work-related materials or to investigate violations of workplace rules—searches of the sort that are regarded as reasonable and normal in the private-employer context—do not violate the ... Amendment," *id.*, at 732, 107 S.Ct. 1492. Pp. 2627 – 2629.

(b) Even assuming that Quon had a reasonable expectation of privacy in his text messages, the search was reasonable under both *O'Connor* approaches, the plurality's and Justice SCALIA's. Pp. 2629 – 2633.

***748** (1) The Court does not resolve the parties' disagreement over Quon's privacy expectation. Prudence counsels caution before the facts in this case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations of employees using employer-provided communication devices. Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve. Because it is therefore preferable to dispose of this case on narrower grounds, the Court assumes, *arguendo*, that: (1) Quon had a reasonable privacy expectation; (2) petitioners' review of the transcript constituted a Fourth Amendment search; and (3) the principles applicable to a government employer's search of an employee's physical office apply as well in the electronic sphere. Pp. 2629 – 2630.

(2) Petitioners' warrantless review of Quon's pager transcript was reasonable under the *O'Connor* plurality's approach because it was motivated by a legitimate work-related purpose, and because it was not excessive in scope. See 480 U.S., at 726, 107 S.Ct. 1492. There were "reasonable grounds for [finding it] necessary for a noninvestigatory work-related purpose," *ibid.*, in that Chief Scharf had ordered the audit to determine whether the City's contractual character limit was sufficient to meet the City's needs. It was also "reasonably related to the objectives of the search," *ibid.*, because both the City and OPD had a legitimate interest in ensuring that employees were not being forced to pay out of their own pockets for work-related expenses, or, on the other hand, that the City was not paying for extensive personal communications. Reviewing the transcripts was an efficient and expedient way to determine whether either of these factors caused Quon's overages. And the review was also not "excessively intrusive." *Ibid.* Although Quon had exceeded his monthly allotment a number of times, OPD requested transcripts for only August and September 2002 in order to obtain a large enough sample to decide the character limits' efficaciousness,

and all the messages that Quon sent while off duty were redacted. And from OPD's perspective, the fact that Quon likely had only a limited privacy expectation lessened the risk that the review would intrude on highly private details of Quon's life. Similarly, because the City had a legitimate reason for the search and it was not excessively intrusive in light of that justification, the search would be "regarded as reasonable and normal in the private-employer context" and thereby satisfy the approach of Justice SCALIA's concurrence, *id.*, at 732, 107 S.Ct. 1492. ****2624** Conversely, the Ninth Circuit's "least intrusive" means approach was inconsistent with ***749** controlling precedents. See, *e.g.*, *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 663, 115 S.Ct. 2386, 132 L.Ed.2d 564. Pp. 2630 – 2633.

(c) Whether the other respondents can have a reasonable expectation of privacy in their text messages to Quon need not be resolved. They argue that because the search was unreasonable as to Quon, it was also unreasonable as to them, but they make no corollary argument that the search, if reasonable as to Quon, could nonetheless be unreasonable as to them. Given this litigating position and the Court's conclusion that the search was reasonable as to Quon, these other respondents cannot prevail. P. 2633.

529 F.3d 892, reversed and remanded.

KENNEDY, J., delivered the opinion of the Court, in which ROBERTS, C.J., and STEVENS, THOMAS, GINSBURG, BREYER, ALITO, and SOTOMAYOR, JJ., joined, and in which SCALIA, J., joined except for Part III–A. STEVENS, J., filed a concurring opinion. SCALIA, J., filed an opinion concurring in part and concurring in the judgment.
Kent L. Richland (argued), Los Angeles, CA, for the petitioners.

Neal K. Katyal, for the U.S. as amicus curiae, by special leave of the Court, supporting the petitioners.

Dieter Dammeier, Upland, CA, for respondents.

Dimitrios C. Rinos, Rinos & Martin, LLP, Tustin, CA, Kent L. Richland, Kent J. Bullard, Greines, Martin, Stein & Richland LLP, Los Angeles, CA, for Petitioners.

Dimitrios C. Rinos, Rinos & Martin, LLP, Tustin, CA, Kent L. Richland, Kent J. Bullard, Greines, Martin, Stein & Richland LLP, Los Angeles, CA, for Petitioners.

Dieter C. Dammeier, Michael A. McGill, Lackie, Dammeier & McGill, Upland, CA, for Respondents Jerilyn Quon, April Florio, Jeff Quon and Steve Trujillo.

For U.S. Supreme Court Briefs, see:2010 WL 565207 (Pet.Brief)2010 WL 989696 (Resp.Brief)2010 WL 1477819 (Reply.Brief)

Justice KENNEDY delivered the opinion of the Court.

***750** This case involves the assertion by a government employer of the right, in circumstances to be described, to read text messages sent and received on a pager the employer owned and issued to an employee. The employee contends that the privacy of the messages is protected by the ban on " unreasonable searches and seizures" found in the Fourth Amendment to the United States Constitution, made applicable to the States by the Due Process Clause of the Fourteenth Amendment. *Mapp v. Ohio*, 367 U.S. 643, 81 S.Ct. 1684, 6 L.Ed.2d 1081 (1961). Though the case touches issues of farreaching significance, the Court concludes it can be resolved by settled principles determining when a search is reasonable.

I

A

The City of Ontario (City) is a political subdivision of the State of California. The case arose out of

incidents in 2001 and 2002 when respondent Jeff Quon was employed by the Ontario Police Department (OPD). He was a police sergeant and member of OPD's Special Weapons and Tactics (SWAT) Team. The City, OPD, and OPD's Chief, Lloyd Scharf, are petitioners****2625** here. As will be discussed, two respondents share the last name Quon. In this opinion "Quon" refers to Jeff Quon, for the relevant events mostly revolve around him.

In October 2001, the City acquired 20 alphanumeric pagers capable of sending and receiving text messages. Arch Wireless Operating Company provided wireless service for the pagers. Under the City's service contract with Arch Wireless, each pager was allotted a limited number of characters ***751** sent or received each month. Usage in excess of that amount would result in an additional fee. The City issued pagers to Quon and other SWAT Team members in order to help the SWAT Team mobilize and respond to emergency situations.

Before acquiring the pagers, the City announced a "Computer Usage, Internet and E–Mail Policy" (Computer Policy) that applied to all employees. Among other provisions, it specified that the City "reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources." App. to Pet. for Cert. 152a. In March 2000, Quon signed a statement acknowledging that he had read and understood the Computer Policy.

The Computer Policy did not apply, on its face, to text messaging. Text messages share similarities with e-mails, but the two differ in an important way. In this case, for instance, an e-mail sent on a City computer was transmitted through the City's own data servers, but a text message sent on one of the City's pagers was transmitted using wireless radio frequencies from an individual pager to a receiving station owned by Arch Wireless. It was routed through Arch Wireless' computer network, where it remained until the recipient's pager or cellular telephone was ready to receive the message, at which point Arch Wireless transmitted the message from the transmitting station nearest to the recipient. After delivery, Arch Wireless retained a copy on its computer servers. The message did not pass through computers owned by the City.

Although the Computer Policy did not cover text messages by its explicit terms, the City made clear to employees, including Quon, that the City would treat text messages the same way as it treated e-mails. At an April 18, 2002, staff meeting at which Quon was present, Lieutenant Steven Duke, the OPD officer responsible for the City's contract ***752** with Arch Wireless, told officers that messages sent on the pagers "are considered e-mail messages. This means that [text] messages would fall under the City's policy as public information and [would be] eligible for auditing." App. 30. Duke's comments were put in writing in a memorandum sent on April 29, 2002, by Chief Scharf to Quon and other City personnel.

Within the first or second billing cycle after the pagers were distributed, Quon exceeded his monthly text message character allotment. Duke told Quon about the overage, and reminded him that messages sent on the pagers were "considered e-mail and could be audited." *Id.*, at 40. Duke said, however, that "it was not his intent to audit [an] employee's text messages to see if the overage [was] due to work related transmissions." *Ibid.* Duke suggested that Quon could reimburse the City for the overage fee rather than have Duke audit the messages. Quon wrote a check to the City for the overage. Duke offered the same arrangement to other employees who incurred overage fees.

Over the next few months, Quon exceeded his character limit three or four times. Each time he reimbursed the City. Quon ****2626** and another officer

again incurred overage fees for their pager usage in August 2002. At a meeting in October, Duke told Scharf that he had become " 'tired of being a bill collector.' " *Id.*, at 91. Scharf decided to determine whether the existing character limit was too low—that is, whether officers such as Quon were having to pay fees for sending work-related messages—or if the overages were for personal messages. Scharf told Duke to request transcripts of text messages sent in August and September by Quon and the other employee who had exceeded the character allowance.

At Duke's request, an administrative assistant employed by OPD contacted Arch Wireless. After verifying that the City was the subscriber on the accounts, Arch Wireless provided the desired transcripts. Duke reviewed the transcripts***753** and discovered that many of the messages sent and received on Quon's pager were not work related, and some were sexually explicit. Duke reported his findings to Scharf, who, along with Quon's immediate supervisor, reviewed the transcripts himself. After his review, Scharf referred the matter to OPD's internal affairs division for an investigation into whether Quon was violating OPD rules by pursuing personal matters while on duty.

The officer in charge of the internal affairs review was Sergeant Patrick McMahon. Before conducting a review, McMahon used Quon's work schedule to redact the transcripts in order to eliminate any messages Quon sent while off duty. He then reviewed the content of the messages Quon sent during work hours. McMahon's report noted that Quon sent or received 456 messages during work hours in the month of August 2002, of which no more than 57 were work related; he sent as many as 80 messages during a single day at work; and on an average workday, Quon sent or received 28 messages, of which only 3 were related to police business. The report concluded that Quon had violated OPD rules. Quon was allegedly disciplined.

B

Raising claims under Rev. Stat. § 1979, 42 U.S.C. § 1983; 18 U.S.C. § 2701 *et seq.*, popularly known as the Stored Communications Act (SCA); and California law, Quon filed suit against petitioners in the United States District Court for the Central District of California. Arch Wireless and an individual not relevant here were also named as defendants. Quon was joined in his suit by another plaintiff who is not a party before this Court and by the other respondents, each of whom exchanged text messages with Quon during August and September 2002: Jerilyn Quon, Jeff Quon's then-wife, from whom he was separated; April Florio, an OPD employee with whom Jeff Quon was romantically involved; and Steve Trujillo, another member of the OPD SWAT Team. ***754** Among the allegations in the complaint was that petitioners violated respondents' Fourth Amendment rights and the SCA by obtaining and reviewing the transcript of Jeff Quon's pager messages and that Arch Wireless had violated the SCA by turning over the transcript to the City.

The parties filed cross-motions for summary judgment. The District Court granted Arch Wireless' motion for summary judgment on the SCA claim but denied petitioners' motion for summary judgment on the Fourth Amendment claims. *Quon v. Arch Wireless Operating Co.*, 445 F.Supp.2d 1116 (C.D.Cal.2006). Relying on the plurality opinion in *O'Connor v. Ortega*, 480 U.S. 709, 711, 107 S.Ct. 1492, 94 L.Ed.2d 714 (1987), the District Court determined that Quon had a reasonable expectation of privacy in the content of his text messages. Whether the audit of the****2627** text messages was nonetheless reasonable, the District Court concluded, turned on Chief Scharf's intent: "[I]f the purpose for the audit was to determine if Quon was using his pager to 'play games' and 'waste time,' then the audit was not constitutionally reasonable"; but if the audit's purpose "was to determine the efficacy of the existing character limits to ensure that officers were not paying hidden work-related costs, ... no

constitutional violation occurred." 445 F.Supp.2d, at 1146.

The District Court held a jury trial to determine the purpose of the audit. The jury concluded that Scharf ordered the audit to determine the efficacy of the character limits. The District Court accordingly held that petitioners did not violate the Fourth Amendment. It entered judgment in their favor.

The United States Court of Appeals for the Ninth Circuit reversed in part. 529 F.3d 892 (2008). The panel agreed with the District Court that Jeff Quon had a reasonable expectation of privacy in his text messages but disagreed with the District Court about whether the search was reasonable. Even though the search was conducted for "a legitimate work-related rationale***755** ," the Court of Appeals concluded, it "was not reasonable in scope." *Id.*, at 908. The panel disagreed with the District Court's observation that "there were no less-intrusive means" that Chief Scharf could have used "to verify the efficacy of the 25,000 character limit ... without intruding on [respondents'] Fourth Amendment rights." *Id.*, at 908–909. The opinion pointed to a "host of simple ways" that the chief could have used instead of the audit, such as warning Quon at the beginning of the month that his future messages would be audited, or asking Quon himself to redact the transcript of his messages. *Id.*, at 909. The Court of Appeals further concluded that Arch Wireless had violated the SCA by turning over the transcript to the City.

The Ninth Circuit denied a petition for rehearing en banc. ***Quon v. Arch Wireless Operating Co.*, 554 F. 3d 769 (2009)**. Judge Ikuta, joined by six other Circuit Judges, dissented. ***Id.*, at 774– 779**. Judge Wardlaw concurred in the denial of rehearing, defending the panel's opinion against the dissent. ***Id.*, at 769– 774**.

This Court granted the petition for certiorari filed by the City, OPD, and Chief Scharf challenging the Court of Appeals' holding that they violated the Fourth Amendment. 558 U.S. 1090, 130 S.Ct. 1011, 175 L.Ed.2d 617 (2009). The petition for certiorari filed by Arch Wireless challenging the Ninth Circuit's ruling that Arch Wireless violated the SCA was denied. *USA Mobility Wireless, Inc. v. Quon*, 558 U.S. 1091, 130 S.Ct. 1011, 175L.Ed.2d 618 (2009).

II

[1][2][3] The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated ...." It is well settled that the Fourth Amendment's protection extends beyond the sphere of criminal investigations. *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 530, 87 S.Ct. 1727, 18 L.Ed.2d 930 (1967). "The Amendment guarantees the privacy, dignity, and security of ***756** persons against certain arbitrary and invasive acts by officers of the Government," without regard to whether the government actor is investigating crime or performing another function. *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602, 613–614, 109 S.Ct. 1402, 103 L.Ed.2d 639 (1989). The Fourth Amendment applies as well when the Government acts in its capacity as an employer. ****2628***Treasury Employees v. Von Raab*, 489 U.S. 656, 665, 109 S.Ct. 1384, 103 L.Ed.2d 685 (1989).

[4] The Court discussed this principle in *O'Connor*. There a physician employed by a state hospital alleged that hospital officials investigating workplace misconduct had violated his Fourth Amendment rights by searching his office and seizing personal items from his desk and filing cabinet. All Members of the Court agreed with the general principle that "[i]ndividuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer." 480 U.S., at 717, 107 S.Ct. 1492 (plurality opinion); see also *id.*, at 731, 107 S.Ct.

1492 (SCALIA, J., concurring in judgment); *id.*, at 737, 107 S.Ct. 1492 (Blackmun, J., dissenting). A majority of the Court further agreed that " 'special needs, beyond the normal need for law enforcement,' " make the warrant and probable-cause requirement impracticable for government employers. *Id.*, at 725, 107 S.Ct. 1492 (plurality opinion) (quoting *New Jersey v. T.L. O.*, 469 U.S. 325, 351, 105 S.Ct. 733, 83 L.Ed.2d 720 (1985)) (Blackmun, J., concurring in judgment); 480 U.S., at 732, 107 S.Ct. 1492 (opinion of SCALIA, J.) (quoting same).

[5][6] The *O'Connor* Court did disagree on the proper analytical framework for Fourth Amendment claims against government employers. A four-Justice plurality concluded that the correct analysis has two steps. First, because "some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable," *id.*, at 718, 107 S.Ct. 1492, a court must consider "[t]he operational realities of the workplace" in order to determine whether an employee's Fourth Amendment rights are implicated, *id.*, at 717, 107 S.Ct. 1492. On this view, "the question whether an employee has a reasonable***757** expectation of privacy must be addressed on a case-by-case basis." *Id.*, at 718, 107 S.Ct. 1492. Next, where an employee has a legitimate privacy expectation, an employer's intrusion on that expectation "for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances." *Id.*, at 725–726, 107 S.Ct. 1492.

[7] Justice SCALIA, concurring in the judgment, outlined a different approach. His opinion would have dispensed with an inquiry into "operational realities" and would conclude "that the offices of government employees ... are covered by Fourth Amendment protections as a general matter." *Id.*, at 731, 107 S.Ct. 1492. But he would also have held "that government searches to retrieve work-related materials or to investigate violations of workplace rules—searches of the sort that are regarded as reasonable and normal in the private-employer context—do not violate the Fourth Amendment." *Id.*, at 732, 107 S.Ct. 1492.

Later, in the *Von Raab* decision, the Court explained that "operational realities" could diminish an employee's privacy expectations, and that this diminution could be taken into consideration when assessing the reasonableness of a workplace search. 489 U.S., at 671, 109 S.Ct. 1384. In the two decades since *O'Connor*, however, the threshold test for determining the scope of an employee's Fourth Amendment rights has not been clarified further. Here, though they disagree on whether Quon had a reasonable expectation of privacy, both petitioners and respondents start from the premise that the *O'Connor* plurality controls. See Brief for Petitioners 22–28; Brief for Respondents 25–32. It is not necessary to resolve whether that premise is correct. The case can be decided by determining that the search was ****2629** reasonable even assuming Quon had a reasonable expectation of privacy. The two *O'Connor* approaches—the plurality's and Justice SCALIA's—therefore lead to the same result here.

***758** III

A

Before turning to the reasonableness of the search, it is instructive to note the parties' disagreement over whether Quon had a reasonable expectation of privacy. The record does establish that OPD, at the outset, made it clear that pager messages were not considered private. The City's Computer Policy stated that "[u]sers should have no expectation of privacy or confidentiality when using" City computers. App. to Pet. for Cert. 152a. Chief Scharf's memo and Duke's statements made clear that this official policy extended to text messaging. The disagreement, at least as respondents see the case, is over whether Duke's later statements overrode the official policy. Respondents contend that because Duke told Quon that an audit would be unnecessary if Quon paid for the overage, Quon reasonably could expect that the contents of his messages would remain private.

At this point, were we to assume that inquiry into "operational realities" were called for, compare *O'Connor*, 480 U.S., at 717, 107 S.Ct. 1492 (plurality opinion), with *id.*, at 730–731, 107 S.Ct. 1492 (opinion of SCALIA, J.); see also *id.*, at 737–738, 107 S.Ct. 1492 (BLACKMUN, J., dissenting), it would be necessary to ask whether Duke's statements could be taken as announcing a change in OPD policy, and if so, whether he had, in fact or appearance, the authority to make such a change and to guarantee the privacy of text messaging. It would also be necessary to consider whether a review of messages sent on police pagers, particularly those sent while officers are on duty, might be justified for other reasons, including performance evaluations, litigation concerning the lawfulness of police actions, and perhaps compliance with state open records laws. See Brief for Petitioners 35–40 (citing Cal. Public Records Act, Cal. Govt.Code Ann. § 6250 *et seq.* (West 2008)). These matters would all bear on the legitimacy of an employee's privacy expectation.

[8] ***759** The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. See, *e.g.*, *Olmstead v. United States*, 277 U.S. 438, 48 S.Ct. 564, 72 L.Ed. 944 (1928), overruled by *Katz v. United States*, 389 U.S. 347, 353, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967). In *Katz*, the Court relied on its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth. See *id.*, at 360–361, 88 S.Ct. 507 (Harlan, J., concurring). It is not so clear that courts at present are on so sure a ground. Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices.

Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. As one *amici* brief notes, many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency. See Brief for Electronic Frontier ****2630** Foundation et al. 16–20. Another *amicus* points out that the law is beginning to respond to these developments, as some States have recently passed statutes requiring employers to notify employees when monitoring their electronic communications. See Brief for New York Intellectual Property Law Association 22 (citing Del.Code Ann., Tit. 19, § 705 (2005); Conn. Gen.Stat. Ann. § 31–48d (West 2003)). At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve.

Even if the Court were certain that the *O'Connor* plurality's approach were the right one, the Court would have difficulty predicting how employees' privacy expectations will be shaped by those changes or the degree to which society ***760** will be prepared to recognize those expectations as reasonable. See 480 U.S., at 715, 107 S.Ct. 1492. Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.

A broad holding concerning employees' privacy expectations vis–à-vis employer-provided technolo-

gical equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds. For present purposes we assume several propositions *arguendo:* First, Quon had a reasonable expectation of privacy in the text messages sent on the pager provided to him by the City; second, petitioners' review of the transcript constituted a search within the meaning of the Fourth Amendment; and third, the principles applicable to a government employer's search of an employee's physical office apply with at least the same force when the employer intrudes on the employee's privacy in the electronic sphere.

B

[9] Even if Quon had a reasonable expectation of privacy in his text messages, petitioners did not necessarily violate the Fourth Amendment by obtaining and reviewing the transcripts. Although as a general matter, warrantless searches "are *per se* unreasonable under the Fourth Amendment," there are "a few specifically established and well-delineated exceptions" to that general rule. *Katz, supra,* at 357, 88 S.Ct. 507. The Court has held that the " 'special needs' " of the workplace ***761** justify one such exception. *O'Connor,* 480 U.S., at 725, 107 S.Ct. 1492 (plurality opinion); *id.,* at 732, 107 S.Ct. 1492 (SCALIA, J., concurring in judgment); *Von Raab,* 489 U.S., at 666–667, 109 S.Ct. 1384.

Under the approach of the *O'Connor* plurality, when conducted for a "noninvestigatory, work-related purpos[e]" or for the "investigatio[n] of work-related misconduct," a government employer's warrantless search is reasonable if it is " 'justified at its inception' " and if " 'the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of' " the circumstances giving rise to the search. 480 U.S., at 725–726, 107 S.Ct. 1492. The search here satisfied the standard of the *O'Connor* plurality and was reasonable under that approach.

****2631** The search was justified at its inception because there were "reasonable grounds for suspecting that the search [was] necessary for a noninvestigatory work-related purpose." *Id.,* at 726, 107 S.Ct. 1492. As a jury found, Chief Scharf ordered the search in order to determine whether the character limit on the City's contract with Arch Wireless was sufficient to meet the City's needs. This was, as the Ninth Circuit noted, a "legitimate work-related rationale." 529 F.3d, at 908. The City and OPD had a legitimate interest in ensuring that employees were not being forced to pay out of their own pockets for work-related expenses, or on the other hand that the City was not paying for extensive personal communications.

As for the scope of the search, reviewing the transcripts was reasonable because it was an efficient and expedient way to determine whether Quon's overages were the result of work-related messaging or personal use. The review was also not " 'excessively intrusive.' " *O'Connor, supra,* at 726, 107 S.Ct. 1492 (plurality opinion). Although Quon had gone over his monthly allotment a number of times, OPD requested transcripts for only the months of August and September 2002. While it may have been reasonable as well for OPD to review transcripts of all the months in which Quon exceeded his ***762** allowance, it was certainly reasonable for OPD to review messages for just two months in order to obtain a large enough sample to decide whether the character limits were efficacious. And it is worth noting that during his internal affairs investigation, McMahon redacted all messages Quon sent while off duty, a measure which reduced the intrusiveness of any further review of the transcripts.

Furthermore, and again on the assumption that Quon had a reasonable expectation of privacy in the contents of his messages, the extent of an expectation is relevant to assessing whether the search was too intrusive. See *Von Raab, supra,* at 671, 109 S.Ct. 1384; cf. *Vernonia School Dist. 47J v. Acton,* 515 U.S. 646, 654–657, 115 S.Ct. 2386, 132 L.Ed.2d 564

(1995). Even if he could assume some level of privacy would inhere in his messages, it would not have been reasonable for Quon to conclude that his messages were in all circumstances immune from scrutiny. Quon was told that his messages were subject to auditing. As a law enforcement officer, he would or should have known that his actions were likely to come under legal scrutiny, and that this might entail an analysis of his on-the-job communications. Under the circumstances, a reasonable employee would be aware that sound management principles might require the audit of messages to determine whether the pager was being appropriately used. Given that the City issued the pagers to Quon and other SWAT Team members in order to help them more quickly respond to crises—and given that Quon had received no assurances of privacy—Quon could have anticipated that it might be necessary for the City to audit pager messages to assess the SWAT Team's performance in particular emergency situations.

From OPD's perspective, the fact that Quon likely had only a limited privacy expectation, with boundaries that we need not here explore, lessened the risk that the review would intrude on highly private details of Quon's life. OPD's audit of messages on Quon's employer-provided pager was not nearly as intrusive as a search of his personal e-mail account ***763** or pager, or a wiretap on his home phone line, would have been. That the search did reveal intimate details of Quon's life does not make it unreasonable, for under the circumstances a reasonable employer would not expect that such a review would intrude****2632** on such matters. The search was permissible in its scope.

The Court of Appeals erred in finding the search unreasonable. It pointed to a "host of simple ways to verify the efficacy of the 25,000 character limit ... without intruding on [respondents'] Fourth Amendment rights." 529 F.3d, at 909. The panel suggested that Scharf "could have warned Quon that for the month of September he was forbidden from using his pager for personal communications, and that the contents of all his messages would be reviewed to ensure the pager was used only for work-related purposes during that time frame. Alternatively, if [OPD] wanted to review past usage, it could have asked Quon to count the characters himself, or asked him to redact personal messages and grant permission to [OPD] to review the redacted transcript." *Ibid.*

[10] This approach was inconsistent with controlling precedents. This Court has "repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment." *Vernonia, supra,* at 663, 115 S.Ct. 2386; see also, *e.g., Board of Ed. of Independent School Dist. No. 92 of Pottawatomie Cty. v. Earls,*536 U.S. 822, 837, 122 S.Ct. 2559, 153 L.Ed.2d 735 (2002); *Illinois v. Lafayette,* 462 U.S. 640, 647, 103 S.Ct. 2605, 77 L.Ed.2d 65 (1983). That rationale "could raise insuperable barriers to the exercise of virtually all search-and-seizure powers," *United States v. Martinez–Fuerte,* 428 U.S. 543, 557, n. 12, 96 S.Ct. 3074, 49 L.Ed.2d 1116 (1976), because "judges engaged in *post hoc* evaluations of government conduct can almost always imagine some alternative means by which the objectives of the government might have been accomplished," *Skinner,* 489 U.S., at 629, n. 9, 109 S.Ct. 1402 (internal quotation marks and brackets omitted). The analytic errors of the Court of Appeals in this case illustrate the necessity of ***764** this principle. Even assuming there were ways that OPD could have performed the search that would have been less intrusive, it does not follow that the search as conducted was unreasonable.

Respondents argue that the search was *per se* unreasonable in light of the Court of Appeals' conclusion that Arch Wireless violated the SCA by giving the City the transcripts of Quon's text messages. The merits of the SCA claim are not before us. But even if the Court of Appeals was correct to conclude that the SCA forbade Arch Wireless from turning over the transcripts, it does not follow that petitioners' actions were unreasonable. Respondents point to no authority

for the proposition that the existence of statutory protection renders a search *per se* unreasonable under the Fourth Amendment. And the precedents counsel otherwise. See *Virginia v. Moore*, 553 U.S. 164, 168, 128 S.Ct. 1598, 170 L.Ed.2d 559 (2008) (search incident to an arrest that was illegal under state law was reasonable); *California v. Greenwood*, 486 U.S. 35, 43, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988) (rejecting argument that if state law forbade police search of individual's garbage the search would violate the Fourth Amendment). Furthermore, respondents do not maintain that any OPD employee either violated the law him– or herself or knew or should have known that Arch Wireless, by turning over the transcript, would have violated the law. The otherwise reasonable search by OPD is not rendered unreasonable by the assumption that Arch Wireless violated the SCA by turning over the transcripts.

[11] Because the search was motivated by a legitimate work-related purpose, and because it was not excessive in scope, the search was reasonable under the approach of the *O'Connor* plurality. ****2633**480 U.S., at 726, 107 S.Ct. 1492. For these same reasons—that the employer had a legitimate reason for the search, and that the search was not excessively intrusive in light of that justification—the Court also concludes that the search would be "regarded as reasonable and normal in the private-employer context" and would satisfy the approach of Justice ***765** SCALIA's concurrence. *Id.*, at 732, 107 S.Ct. 1492. The search was reasonable, and the Court of Appeals erred by holding to the contrary. Petitioners did not violate Quon's Fourth Amendment rights.

C

Finally, the Court must consider whether the search violated the Fourth Amendment rights of Jerilyn Quon, Florio, and Trujillo, the respondents who sent text messages to Jeff Quon. Petitioners and respondents disagree whether a sender of a text message can have a reasonable expectation of privacy in a message he knowingly sends to someone's employer-provided pager. It is not necessary to resolve this question in order to dispose of the case, however. Respondents argue that because "the search was unreasonable as to Sergeant Quon, it was also unreasonable as to his correspondents." Brief for Respondents 60 (some capitalization omitted; boldface deleted). They make no corollary argument that the search, if reasonable as to Quon, could nonetheless be unreasonable as to Quon's correspondents. See *id.*, at 65–66. In light of this litigating position and the Court's conclusion that the search was reasonable as to Jeff Quon, it necessarily follows that these other respondents cannot prevail.

* * *

Because the search was reasonable, petitioners did not violate respondents' Fourth Amendment rights, and the court below erred by concluding otherwise. The judgment of the Court of Appeals for the Ninth Circuit is reversed, and the case is remanded for further proceedings consistent with this opinion.

It is so ordered.

Justice STEVENS, concurring.

Although I join the Court's opinion in full, I write separately to highlight that the Court has sensibly declined to resolve whether the plurality opinion in ***766***O'Connor v. Ortega*, 480 U.S. 709, 107 S.Ct. 1492, 94 L.Ed.2d 714 (1987), provides the correct approach to determining an employee's reasonable expectation of privacy. See *ante*, at 2628 – 2629. Justice Blackmun, writing for the four dissenting Justices in *O'Connor*, agreed with Justice SCALIA that an employee enjoys a reasonable expectation of privacy in his office. 480 U.S., at 737, 107 S.Ct. 1492. But he advocated a third approach to the reasonable expectation of privacy inquiry, separate from those proposed by the *O'Connor* plurality and by Justice SCALIA, see *ante*, at 2628. Recognizing that it is particularly important to safeguard "a public employee's expectation of privacy in the workplace" in

light of the " reality of work in modern time," 480 U.S., at 739, 107 S.Ct. 1492, which lacks "tidy distinctions" between workplace and private activities, *ibid.*, Justice Blackmun argued that "the precise extent of an employee's expectation of privacy often turns on the nature of the search," *id.*, at 738, 107 S.Ct. 1492. And he emphasized that courts should determine this expectation in light of the specific facts of each particular search, rather than by announcing a categorical standard. See *id.*, at 741, 107 S.Ct. 1492.

For the reasons stated at page 2631 of the Court's opinion, it is clear that respondent Jeff Quon, as a law enforcement officer who served on a SWAT Team, should ****2634** have understood that all of his work-related actions—including all of his communications on his official pager—were likely to be subject to public and legal scrutiny. He therefore had only a limited expectation of privacy in relation to this particular audit of his pager messages. Whether one applies the reasoning from Justice O'Connor's opinion, Justice SCALIA's concurrence, or Justice Blackmun's dissent [FN*] in *O'Connor*, the result ***767** is the same: The judgment of the Court of Appeals in this case must be reversed.

FN* I do not contend that Justice Blackmun's opinion is controlling under *Marks v. United States*, 430 U.S. 188, 193, 97 S.Ct. 990, 51 L.Ed.2d 260 (1977), but neither is his approach to evaluating a reasonable expectation of privacy foreclosed by *O'Connor*. Indeed, his approach to that inquiry led to the conclusion, shared by Justice SCALIA but not adopted by the *O'Connor* plurality, that an employee had a reasonable expectation of privacy in his office. See *O'Connor v. Ortega*, 480 U.S. 709, 718, 107 S.Ct. 1492, 94 L.Ed.2d 714 (1987) (plurality opinion). But Justice Blackmun would have applied the Fourth Amendment's warrant and probable-cause requirements to workplace investigatory searches, *id.*, at 732, 107 S.Ct. 1492 (dissenting opinion), whereas a majority of the Court rejected that view, see *id.*, at 722, 725, 107 S.Ct. 1492 (plurality opinion); *id.*, at 732, 107 S.Ct. 1492 (SCALIA, J., concurring in judgment). It was that analysis—regarding the proper standard for evaluating a search when an employee has a reasonable expectation of privacy—that produced the opposite result in the case. This case does not implicate that debate because it does not involve an investigatory search. The jury concluded that the purpose of the audit was to determine whether the character limits were sufficient for work-related messages. See *ante*, at 2627.

Justice SCALIA, concurring in part and concurring in the judgment.

I join the Court's opinion except for Part III–A. I continue to believe that the "operational realities" rubric for determining the Fourth Amendment's application to public employees invented by the plurality in *O'Connor v. Ortega*, 480 U.S. 709, 717, 107 S.Ct. 1492, 94 L.Ed.2d 714 (1987), is standardless and unsupported. *Id.*, at 729–732, 107 S.Ct. 1492 (SCALIA, J., concurring in judgment). In this case, the proper threshold inquiry should be not whether the Fourth Amendment applies to messages on *public* employees' employer-issued pagers, but whether it applies *in general* to such messages on employer-issued pagers. See *id.*, at 731, 107 S.Ct. 1492.

Here, however, there is no need to answer that threshold question. Even accepting at face value Quon's and his co-plaintiffs' claims that the Fourth Amendment applies to their messages, the city's search was reasonable, and thus did not violate the Amendment. See *id.*, at 726, 107 S.Ct. 1492 (plurality opinion); *id.*, at 732, 107 S.Ct. 1492 (SCALIA, J., concurring in judgment). Since it is unnecessary to decide whether the Fourth Amendment applies, it is unnecessary to resolve which approach in *O'Connor* controls: the plurality's or mine.[FN*] That should end

the matter.

FN* Despite his disclaimer, *ante*, at 2634, n. (concurring opinion), Justice STEVENS' concurrence implies, *ante*, at 2633 – 2634, that it is also an open question whether the approach advocated by Justice Blackmun in his *dissent* in *O'Connor* is the proper standard. There is room for reasonable debate as to which of the two approaches advocated by Justices whose votes supported the judgment in *O'Connor*—the plurality's and mine—is controlling under *Marks v. United States*, 430 U.S. 188, 193, 97 S.Ct. 990, 51 L.Ed.2d 260 (1977). But unless *O'Connor* is overruled, it is assuredly false that a test that would have produced the *opposite* result in that case is still in the running.

***768** The Court concedes as much, *ante*, at 2628 – 2629, 2630 – 2633, yet it inexplicably interrupts its analysis with a recitation of the parties' arguments concerning, and an ****2635** excursus on the complexity and consequences of answering, that admittedly irrelevant threshold question, *ante*, at 2629 – 2630. That discussion is unnecessary. (To whom do we owe an *additional* explanation for declining to decide an issue, once we have explained that it makes no difference?) It also seems to me exaggerated. Applying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we have no choice. The Court's implication, *ante*, at 2629, that where electronic privacy is concerned we should decide less than we otherwise would (that is, less than the principle of law necessary to resolve the case and guide private action)—or that we should hedge our bets by concocting case-specific standards or issuing opaque opinions—is in my view indefensible. The-times-they-are-a-changin' is a feeble excuse for disregard of duty.

Worse still, the digression is self-defeating. Despite the Court's insistence that it is agnostic about the proper test, lower courts will likely read the Court's self-described "instructive" expatiation on how the *O'Connor* plurality's approach would apply here (if it applied), *ante*, at 2629 – 2630, as a heavy-handed hint about how *they* should proceed. Litigants will do likewise, using the threshold question whether the Fourth Amendment is even implicated as a basis for bombarding lower courts with arguments about employer policies, how they were communicated, and whether they were authorized, as well as the latest trends in employees' use of ***769** electronic media. In short, in saying why it is not saying more, the Court says much more than it should.

The Court's inadvertent boosting of the *O'Connor* plurality's standard is all the more ironic because, in fleshing out its fears that applying that test to new technologies will be too hard, the Court underscores the unworkability of that standard. Any rule that requires evaluating whether a given gadget is a "necessary instrumen[t] for self-expression, even self-identification," on top of assessing the degree to which "the law's treatment of [workplace norms has] evolve[d]," *ante*, at 2629 – 2630, is (to put it mildly) unlikely to yield objective answers.

I concur in the Court's judgment.

U.S.,2010.
City of Ontario, Cal. v. Quon
560 U.S. 746, 130 S.Ct. 2619, 93 Empl. Prac. Dec. P 43,907, 177 L.Ed.2d 216, 78 USLW 4591, 159 Lab.Cas. P 61,011, 30 IER Cases 1345, 10 Cal. Daily Op. Serv. 7565, 2010 Daily Journal D.A.R. 9072, 22 Fla. L. Weekly Fed. S 470

END OF DOCUMENT

551 F.Supp.2d 1183, 27 IER Cases 657
(Cite as: 551 F.Supp.2d 1183)

H

United States District Court,
S.D. California.
Vance HILDERMAN, an individual; Highrely Inc., a Delaware corporation, Plaintiffs,
v.
ENEA TEKSCI, INC., dba Enea embedded technology, Defendants.
and Related Counterclaims.

No. 05cv1049 BTM(AJB).
March 12, 2008.

Background: Founder and his engineering software services corporation sued former employer in competing software consulting business, asserting claims for declaratory relief, breach of contract, interference with contractual relations and prospective economic advantage, and violation of state law unfair business practices by wrongfully telling clients that founder had violated severance agreement and was subject to non-compete agreement. Former employer counterclaimed and filed third-party complaint against another former employee, who had been fired and also joined founder's corporation, asserting claims for breach of duty of loyalty, misappropriation of trade secrets, aiding and abetting, breach of contract, conspiracies to intentionally interfere with contract and with prospective economic advantage, and unfair business practices. Former employee counterclaimed for breach of contract, intrusion into private affairs, and violation of Electronic Communications Privacy Act (ECPA) and Stored Communications Act. Parties moved for summary judgment.

Holdings: The District Court, Barry Ted Moskowitz, J., held that:
(1) fact issue remained for founder's claim that former employer breached implied covenant of good faith and fair dealing;
(2) employer did not interfere with customer contracts of founder and corporation;
(3) fact issue remained as to corporation's interference with prospective economic advantage (IPEA) in potential customer contract;
(4) there was no evidence for IPEA claim regarding existing customer contract;
(5) fact issue remained as to unfair trade practices claim against employer;
(6) employer's avionics software processes and checklists were not trade secrets;
(7) employer's customer contact information was not trade secret;
(8) fact issue remained as to whether employer's pricing information was trade secret;
(9) avionics customer's project information was not employer's trade secret;
(10) fact issue remained as to whether employer's customer list was trade secret;
(11) fact issue remained as to misappropriation of employer's trade secret consisting of employee and engineer list;
(12) employer's search of former employee's laptop was not invasion of privacy; and
(13) employer did not violate Stored Communications Act.

Motions granted in part and denied in part.

West Headnotes

[1] Federal Civil Procedure 170A 2470

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)1 In General
170Ak2465 Matters Affecting Right to

Judgment
170Ak2470 k. Absence of genuine issue of fact in general. Most Cited Cases

Federal Civil Procedure 170A 2470.4

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)1 In General
170Ak2465 Matters Affecting Right to Judgment
170Ak2470.4 k. Right to judgment as matter of law. Most Cited Cases

Summary judgment is appropriate if the moving party demonstrates the absence of a genuine issue of material fact and entitlement to judgment as a matter of law. Fed.Rules Civ.Proc.Rule 56, 28 U.S.C.A.

[2] Federal Civil Procedure 170A 2470.1

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)1 In General
170Ak2465 Matters Affecting Right to Judgment
170Ak2470.1 k. Materiality and genuineness of fact issue. Most Cited Cases

On summary judgment motion, a fact is "material" when, under the governing substantive law, it could affect the outcome of the case. Fed.Rules Civ.Proc.Rule 56, 28 U.S.C.A.

[3] Federal Civil Procedure 170A 2470.1

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)1 In General
170Ak2465 Matters Affecting Right to Judgment
170Ak2470.1 k. Materiality and genuineness of fact issue. Most Cited Cases

On summary judgment motion, a dispute is "genuine" if a reasonable jury could return a verdict for the nonmoving party. Fed.Rules Civ.Proc.Rule 56, 28 U.S.C.A.

[4] Federal Civil Procedure 170A 2544

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)3 Proceedings
170Ak2542 Evidence
170Ak2544 k. Burden of proof. Most Cited Cases

A party seeking summary judgment always bears the initial burden of establishing the absence of a genuine issue of material fact. Fed.Rules Civ.Proc.Rule 56, 28 U.S.C.A.

[5] Federal Civil Procedure 170A 2544

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)3 Proceedings
170Ak2542 Evidence
170Ak2544 k. Burden of proof. Most Cited Cases

The party moving for summary judgment can satisfy burden of establishing absence of genuine issue of material fact in two ways: (1) by presenting evidence that negates an essential element of the nonmoving party's case, or (2) by demonstrating that the nonmoving party failed to establish an essential ele-

ment of the nonmoving party's case on which the nonmoving party bears the burden of proving at trial. Fed.Rules Civ.Proc.Rule 56, 28 U.S.C.A.

[6] Federal Civil Procedure 170A 2470.1

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)1 In General
170Ak2465 Matters Affecting Right to Judgment
170Ak2470.1 k. Materiality and genuineness of fact issue. Most Cited Cases

Disputes over irrelevant or unnecessary facts will not preclude a grant of summary judgment. Fed.Rules Civ.Proc.Rule 56, 28 U.S.C.A.

[7] Federal Civil Procedure 170A 2544

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)3 Proceedings
170Ak2542 Evidence
170Ak2544 k. Burden of proof. Most Cited Cases

Once the party moving for summary judgment establishes the absence of genuine issues of material fact, the burden shifts to the nonmoving party to set forth facts showing that a genuine issue of disputed fact remains. Fed.Rules Civ.Proc.Rule 56, 28 U.S.C.A.

[8] Federal Civil Procedure 170A 2544

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)3 Proceedings
170Ak2542 Evidence
170Ak2544 k. Burden of proof. Most Cited Cases

The nonmoving party cannot oppose a properly supported summary judgment motion by resting on mere allegations or denials of his pleadings. Fed.Rules Civ.Proc.Rule 56, 28 U.S.C.A.

[9] Federal Civil Procedure 170A 2543

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)3 Proceedings
170Ak2542 Evidence
170Ak2543 k. Presumptions. Most Cited Cases

When ruling on a summary judgment motion, the court must view all inferences drawn from the underlying facts in the light most favorable to the nonmoving party. Fed.Rules Civ.Proc.Rule 56, 28 U.S.C.A.

[10] Declaratory Judgment 118A 62

118A Declaratory Judgment
118AI Nature and Grounds in General
118AI(D) Actual or Justiciable Controversy
118Ak62 k. Nature and elements in general. Most Cited Cases

The actual controversy requirement of the Declaratory Judgment Act is the same as the case or controversy requirement of Article III. U.S.C.A. Const. Art. 3, § 2, cl. 1; 28 U.S.C. § 2201.

[11] Declaratory Judgment 118A 61

118A Declaratory Judgment
118AI Nature and Grounds in General
118AI(D) Actual or Justiciable Controversy
118Ak61 k. Necessity. Most Cited Cases

Declaratory Judgment 118A 62

118A Declaratory Judgment
118AI Nature and Grounds in General
118AI(D) Actual or Justiciable Controversy
118Ak62 k. Nature and elements in general. Most Cited Cases

Article III requires that there be a substantial controversy of sufficient immediacy and reality to warrant the issuance of a declaratory judgment. U.S.C.A. Const. Art. 3, § 2, cl. 1.

[12] Declaratory Judgment 118A 62

118A Declaratory Judgment
118AI Nature and Grounds in General
118AI(D) Actual or Justiciable Controversy
118Ak62 k. Nature and elements in general. Most Cited Cases

To warrant a declaratory judgment comporting with Article III requirements, an actual controversy must be extant at all stages of review, not merely at the time the complaint is filed. U.S.C.A. Const. Art. 3, § 2, cl. 1.

[13] Declaratory Judgment 118A 145

118A Declaratory Judgment
118AII Subjects of Declaratory Relief
118AII(G) Written Instruments and Contracts
118AII(G)1 In General
118Ak143 Particular Contracts
118Ak145 k. Employment and personal service contracts. Most Cited Cases

Declaration entitling founder of engineering software corporation to solicit business, employees, and customers of former employer after six-month period from date of founder's severance, was not warranted, under Declaratory Judgment Act and Article III case or controversy requirements, since there was no remaining dispute that severance agreement authorized founder's solicitation if he did not use former employer's confidential, proprietary, or trade secret information. U.S.C.A. Const. Art. 3, § 2, cl. 1; 28 U.S.C.A. § 2201.

[14] Federal Civil Procedure 170A 2492

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2492 k. Contract cases in general. Most Cited Cases

There were triable issues as to whether former employee used any confidential, proprietary or trade secret information of his former employer to obtain its customers or employees, precluding summary judgment on his claim that former employer breached parties' severance agreement by falsely telling third parties that he had agreed to non-compete clause and was breaching that agreement by soliciting former employees or customers.

[15] Contracts 95 187(1)

95 Contracts
95II Construction and Operation
95II(B) Parties
95k185 Rights Acquired by Third Persons
95k187 Agreement for Benefit of Third Person
95k187(1) k. In general. Most Cited Cases

Under California law, the circumstance that a literal contract interpretation would result in a benefit to the third party is not enough to entitle that party to demand enforcement; rather, the contracting parties must have intended to confer a benefit on the third party.

[16] Contracts 95 187(1)

95 Contracts
95II Construction and Operation
95II(B) Parties
95k185 Rights Acquired by Third Persons
95k187 Agreement for Benefit of Third Person
95k187(1) k. In general. Most Cited Cases

Under California law, to determine whether a third party is an intended beneficiary entitled to demand enforcement of a contract, or merely an incidental beneficiary not so entitled, involves construction of the parties' intent, gleaned from reading the contract as a whole in light of the circumstances under which it was entered.

[17] Contracts 95 187(1)

95 Contracts
95II Construction and Operation
95II(B) Parties
95k185 Rights Acquired by Third Persons
95k187 Agreement for Benefit of Third Person
95k187(1) k. In general. Most Cited Cases

Founder's engineering software corporation that competed with founder's former employer was not "intended third-party beneficiary" of severance agreement between founder and former employer, under California law, although corporation would benefit from agreement's terms allowing founder to compete with former employer, and thus, corporation lacked standing to assert breach of contract claim against founder's former employer on grounds that parties to agreement could not have intended corporation to be beneficiary of agreement that was entered before corporation was even in existence, and agreement did not mention any future corporations that might be formed.

[18] Corporations and Business Organizations 101 2709

101 Corporations and Business Organizations
101X Mergers, Acquisitions, and Reorganizations
101X(C) Sale, Lease, or Exchange of Substantially All Corporate Assets
101k2705 Agreements to Sell, Lease, or Exchange
101k2709 k. Construction, operation, and effect. Most Cited Cases
(Formerly 101k445)

Under California law, former employee's engineering software corporation that competed with his former employer was not "successor" of former employee, benefited by parties' severance agreement.

[19] Torts 379 242

379 Torts
379III Tortious Interference
379III(B) Business or Contractual Relations
379III(B)2 Particular Cases
379k242 k. Contracts in general. Most Cited Cases

Although engineering software company had its own relationships with competitor's customers, it was outsider to contractual relationships between competitor and those customers, and thus could be held liable,

under California law, if it intentionally interfered with those contracts and prospective contracts.

[20] Federal Civil Procedure 170A 2539

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)3 Proceedings
170Ak2536 Affidavits
170Ak2539 k. Sufficiency of showing. Most Cited Cases

Plaintiff's summary judgment declaration, stating that he was personally aware of contract defendant allegedly interfered with and of fact that it had continued to the present lacked required showing that plaintiff had personal knowledge of these facts.

[21] Torts 379 213

379 Torts
379III Tortious Interference
379III(B) Business or Contractual Relations
379III(B)1 In General
379k213 k. Prospective advantage, contract or relations; expectancy. Most Cited Cases

Under California law, the elements of an interference with prospective economic advantage (IPEA) claim are: (1) an economic relationship between the plaintiff and a third party that carries a probability of future economic benefit to the plaintiff, (2) defendant's knowledge of the relationship, (3) intentional acts on the part of the defendant designed to disrupt the relationship, (4) actual disruption of the relationship, and (5) economic harm to the plaintiff proximately caused by the defendant's acts.

[22] Torts 379 218

379 Torts
379III Tortious Interference
379III(B) Business or Contractual Relations
379III(B)1 In General
379k218 k. Improper means; wrongful, tortious or illegal conduct. Most Cited Cases

Torts 379 255

379 Torts
379III Tortious Interference
379III(B) Business or Contractual Relations
379III(B)3 Actions in General
379k255 k. Pleading. Most Cited Cases

Under California law, for interference with prospective economic advantage (IPEA) claim, the plaintiff must allege that the defendant's act was wrongful by some measure beyond the fact of the interference itself.

[23] Federal Civil Procedure 170A 2515

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2515 k. Tort cases in general. Most Cited Cases

Genuine issue of material fact remained as to whether economic relationship with probability of future economic benefit existed between engineering software corporation and customer that initially stated it would agree to enter contract for engineering services, but later declined to do so due to competitor's allegedly false statements, thus precluding summary judgment on corporation's claim of interference with prospective economic advantage, under California law, based on competitor's allegedly false statements.

[24] Torts 379 218

379 Torts
379III Tortious Interference
379III(B) Business or Contractual Relations
379III(B)1 In General
379k218 k. Improper means; wrongful, tortious or illegal conduct. Most Cited Cases

Under California law, a defendant's act is "independently wrongful," as required for interference with prospective economic advantage (IPEA) claim, if the act is unlawful, that is, if the defendant's act is proscribed by some constitutional, statutory, regulatory, common law, or other determinable legal standard.

[25] Torts 379 218

379 Torts
379III Tortious Interference
379III(B) Business or Contractual Relations
379III(B)1 In General
379k218 k. Improper means; wrongful, tortious or illegal conduct. Most Cited Cases

A violation of California law governing unfair business practices can satisfy the requirement of an independently wrongful act for interference with prospective economic advantage claim.

[26] Torts 379 226

379 Torts
379III Tortious Interference
379III(B) Business or Contractual Relations
379III(B)1 In General
379k226 k. Persons entitled to sue. Most Cited Cases

Torts 379 241

379 Torts
379III Tortious Interference
379III(B) Business or Contractual Relations
379III(B)2 Particular Cases
379k241 k. Business relations or economic advantage, in general. Most Cited Cases

Founder as shareholder of engineering software corporation lacked standing for interference with prospective economic advantage (IPEA) claim, under California law, against founder's former employer based on alleged false statements to customer of founder and his corporation causing refusal to enter potential contract for engineering services, since shareholder could not maintain IPEA claim on own behalf for wrong to corporation by third party based on theory that wrong devalued stock.

[27] Torts 379 241

379 Torts
379III Tortious Interference
379III(B) Business or Contractual Relations
379III(B)2 Particular Cases
379k241 k. Business relations or economic advantage, in general. Most Cited Cases

There was no evidence that founder's engineering software corporation lost existing customer contract due to false statements of founder's former employer, as required for interference with prospective economic advantage claim, under California law, on grounds that former employer allegedly wrongly accused founder of breaching non-compete clause in severance agreement with former employer, since existing customer contract came to end due to lack of funding.

[28] Federal Civil Procedure 170A 2493

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases

170Ak2493 k. Copyright, trademark, and unfair competition cases. Most Cited Cases

Genuine issue of material fact existed as to whether competitor falsely informed customers of engineering services corporation that corporation's founder had stolen competitor's property, while founder was former employee of competitor, and was violating non-compete agreement, thus precluding summary judgment on claim by founder and his corporation that competitor committed unfair business practices in violation of California law. West's Ann.Cal.Bus. & Prof.Code § 17200.

[29] Antitrust and Trade Regulation 29T 420

29T Antitrust and Trade Regulation
29TIV Trade Secrets and Proprietary Information
29TIV(A) In General
29Tk420 k. Particular cases, in general. Most Cited Cases

Engineering software provider's checklists and processes for meeting avionics software testing and certification standards were not "trade secrets," under California law, that derived independent economic value from not being generally known to avionics industry, as required for software provider's claim of misappropriation of trade secrets by competitor and its founder and employee who prepared those processes and checklists from public domain sources while formerly employed by software provider, since provider failed to explain how processes and checklists were different from or improvement on publicly available information other than that checklists better "tracked" public data. West's Ann.Cal.Civ.Code § 3426.1(d).

[30] Estoppel 156 84

156 Estoppel
156III Equitable Estoppel
156III(B) Grounds of Estoppel
156k82 Representations
156k84 k. Matters of fact or of opinion. Most Cited Cases

Estoppel 156 87

156 Estoppel
156III Equitable Estoppel
156III(B) Grounds of Estoppel
156k82 Representations
156k87 k. Relying and acting on representations. Most Cited Cases

Engineering software services corporation and its founder and employee were not estopped, under California law, from denying that competitor's processes and checklists for meeting avionics software testing and certification standards were trade secrets, based on founder's prior statements while employed by competitor indicating that processes and checklists were very unique and proprietary, as required for competitor's misappropriation of trade secrets claim, under California law, since founder's statement was vague puffery without identifying uniqueness, proprietary interest did not constitute trade secret, and provider did not detrimentally rely on statements. West's Ann.Cal.Civ.Code § 3426.1(d); West's Ann.Cal.Evid.Code § 623.

[31] Antitrust and Trade Regulation 29T 420

29T Antitrust and Trade Regulation
29TIV Trade Secrets and Proprietary Information
29TIV(A) In General
29Tk420 k. Particular cases, in general. Most Cited Cases

A proprietary interests in a copyright or other intellectual property does not necessarily constitute "trade secrets."

[32] Estoppel 156 68(4)

156 Estoppel
156III Equitable Estoppel
156III(B) Grounds of Estoppel
156k68 Claim or Position in Judicial Proceedings
156k68(4) k. Defense or objection inconsistent with previous claim or position in general. Most Cited Cases

Founder of engineering software services corporation was not judicially estopped from denying that competitor's processes and checklists for meeting avionics software testing and certification standards were trade secrets, based on founder's allegedly contrary position in prior copyright infringement suit while formerly employed by competitor, as required for competitor's misappropriation of trade secrets claim, under California law, since founder had not taken inconsistent position, but rather, actually defended suit by arguing that information was not trade secret. West's Ann.Cal.Civ.Code § 3426.1(d); West's Ann.Cal.Evid.Code § 623.

[33] United States Magistrates 394 27

394 United States Magistrates
394k24 Review and Supervision by District Court
394k27 k. De novo hearing or review. Most Cited Cases

Claims of discovery abuse not raised before magistrate judge were not reviewable.

[34] Antitrust and Trade Regulation 29T 420

29T Antitrust and Trade Regulation
29TIV Trade Secrets and Proprietary Information
29TIV(A) In General
29Tk420 k. Particular cases, in general. Most Cited Cases

There was no evidence that software consultant's contact information with avionics customer was "trade secret," as required for misappropriation of trade secrets claim, under California law, against competitor and its founder and employee who were formerly employed by consultant, since customer contact person had long-standing professional relationship with employee, and customer frequently directed outside suppliers to contact person and provided his contact information. West's Ann.Cal.Civ.Code § 3426.1(d).

[35] Federal Civil Procedure 170A 2515

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2515 k. Tort cases in general. Most Cited Cases

Genuine issue of material fact existed as to whether software consultant's pricing information was trade secret, under California law, due to pricing differences among various customers, thus precluding summary judgment on consultant's claim that competitor and its founder and employee, who were former employees of consultant, misappropriated trade secrets by using price lists to bid on avionics project at lower price and take business from consultant. West's Ann.Cal.Civ.Code § 3426.1(d).

[36] Antitrust and Trade Regulation 29T 420

29T Antitrust and Trade Regulation
29TIV Trade Secrets and Proprietary Information
29TIV(A) In General
29Tk420 k. Particular cases, in general. Most Cited Cases

Software consultant's information regarding avionics customer's project was not "trade secret," as

required for misappropriation of trade secrets claim, under California law, against competitor and its founder and employee who were formerly employed by consultant, although customer called employee thinking that he was still employed by consultant, since customer's primary purpose in calling was to talk to employee in particular, regardless of who his employer was, due to critical design review for project that had already failed twice, and Air Force had specifically recommended particular employee and founder. West's Ann.Cal.Civ.Code § 3426.1(d).

[37] Federal Civil Procedure 170A 2515

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2515 k. Tort cases in general. Most Cited Cases

Genuine issues of material fact remained as to whether software consultant's avionics customer list derived economic value from not being generally known to public and whether consultant took reasonable steps to keep customer list secret, as required for trade secret, under California law, thus precluding summary judgment as to consultant's misappropriation of trade secrets claim against competitor and its founder and employee who were formerly employed by consultant. West's Ann.Cal.Civ.Code § 3426.1(d).

[38] Antitrust and Trade Regulation 29T 421

29T Antitrust and Trade Regulation
29TIV Trade Secrets and Proprietary Information
29TIV(A) In General
29Tk421 k. Customer lists and information. Most Cited Cases

Client lists can receive trade secret protection if they satisfy the requirements of California law defining trade secrets. West's Ann.Cal.Civ.Code § 3426.1(d).

[39] Antitrust and Trade Regulation 29T 421

29T Antitrust and Trade Regulation
29TIV Trade Secrets and Proprietary Information
29TIV(A) In General
29Tk421 k. Customer lists and information. Most Cited Cases

Under California law governing trade secrets, where the employer has expended time and effort identifying customers with particular needs or characteristics, former employees are prohibited from using this information to capture a share of the market. West's Ann.Cal.Civ.Code § 3426.1(d).

[40] Antitrust and Trade Regulation 29T 421

29T Antitrust and Trade Regulation
29TIV Trade Secrets and Proprietary Information
29TIV(A) In General
29Tk421 k. Customer lists and information. Most Cited Cases

Under California law governing trade secrets, protecting information that derives economic value from not being generally known to the public, a customer list can be found to have economic value because its disclosure would allow a competitor to direct its sales efforts to those customers who have already shown a willingness to use a unique type of service or product, as opposed to a list of people who only might be interested. West's Ann.Cal.Civ.Code § 3426.1(d).

[41] Antitrust and Trade Regulation 29T 419

29T Antitrust and Trade Regulation
29TIV Trade Secrets and Proprietary Information
29TIV(A) In General

29Tk419 k. Vigilance in protecting secret; abandonment or waiver. Most Cited Cases

Under California law governing trade secrets, protecting information that derives economic value from not being generally known to the public, the lack of confidentiality agreements is not dispositive on the issue of secrecy in that an employer may have taken other precautions to keep its information secret, such as verbally telling its clients and employees that the information was confidential or limiting access to information on a "need to know" basis. West's Ann.Cal.Civ.Code § 3426.1(d).

[42] Federal Civil Procedure 170A 2515

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2515 k. Tort cases in general. Most Cited Cases

Genuine issues of material fact remained as to whether software consultant's trade secret information, consisting of employee and engineer list, was used by competitor to solicit new recruits, thus precluding summary judgment as to consultant's misappropriation of trade secrets claim, under California law, against competitor and its founder and employee who were formerly employed by consultant. West's Ann.Cal.Civ.Code § 3426.1(d).

[43] Torts 379 341

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)2 Intrusion
379k341 k. Particular cases in general. Most Cited Cases

Employer's alleged intrusion into former employee's privacy by searching for disclosures of confidential information on company-issued laptop computer, on which employee maintained personal e-mail account with log-in and password stored on laptop, was not "highly offensive," as required for invasion of privacy claim, under Arizona and California law, although employer could have accessed private data from laptop that employee believed he was able to purchase upon leaving company, since computer was still employer's property, search was not motivated by desire to root out private information but to protect confidential data, laptop was kept in locked office and not passed around company, and intrusion was limited to only controller and forensic computer specialist.

[44] Torts 379 340

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)2 Intrusion
379k340 k. In general. Most Cited Cases

Under Arizona and California law, the elements for invasion of privacy are: (1) an intentional intrusion into a private place, conversation, or matter (2) in a manner highly offensive to a reasonable person.

[45] Torts 379 340

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)2 Intrusion
379k340 k. In general. Most Cited Cases

Under Arizona and California law, to prevail on the element of invasion of privacy regarding an intentional intrusion into a private place, conversation, or matter, the plaintiff must show that he had a rea-

551 F.Supp.2d 1183, 27 IER Cases 657
(Cite as: 551 F.Supp.2d 1183)

sonable expectation of seclusion or solitude in the place, conversation, or data source.

[46] Torts 379 340

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)2 Intrusion
379k340 k. In general. Most Cited Cases

Under Arizona and California law, in determining whether an alleged invasion of privacy is highly offensive, relevant considerations include the degree of the intrusion, the context, conduct, and circumstances surrounding the intrusion, as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded.

[47] Telecommunications 372 1342

372 Telecommunications
372VIII Computer Communications
372k1339 Civil Liabilities; Illegal or Improper Purposes
372k1342 k. Fraud; unauthorized access or transmission. Most Cited Cases

Employee's storage of personal and private e-mail messages on hard drive of company-issued laptop computer did not constitute "electronic storage," within meaning of Stored Communications Act, prohibiting unauthorized access of wire or electronic communication while in electronic storage in facility providing electronic communication service, as required for claim that employer violated Act by accessing employee's e-mails, since stored e-mails were not in temporary intermediate storage and were not stored by electronic communication service for purpose of backup protection. 18 U.S.C.A. §§ 2510(17), 2701(a)(1).

***1190** Fletcher W. Paddison, Malte L. Farnaes, Ross Dixon and Bell, San Diego, CA, for Plaintiffs.

Adron W. Beene, Law Offices of Adron W. Beene, San Jose, CA, for Defendants.

ORDER (1) GRANTING IN PART AND DENYING IN PART ENEA'S MOTION FOR SUMMARY JUDGMENT (2) GRANTING IN PART AND DENYING IN PART COUNTERDEFENDANTS' FIRST MOTION FOR PARTIAL SUMMARY JUDGMENT; (3) DENYING COUNTERDEFENDANTS' SECOND MOTION FOR PARTIAL SUMMARY JUDGMENT; AND (4) GRANTING ENEA'S MOTION FOR SUMMARY JUDGMENT ON THE SECOND AND THIRD CLAIMS OF BAGHAI'S COUNTERCLAIM

BARRY TED MOSKOWITZ, District Judge.

Defendant Enea TekSci, Inc. ("Enea") has filed a motion for summary judgment on the Complaint filed by Vance Hilderman ("Hilderman") and Highrely, Inc. ("Highrely") (collectively "Plaintiffs"). Hilderman, Highrely, and Tony Baghai ("Baghai") (collectively "Counterdefendants") have filed two motions for partial summary judgment on Enea's counterclaims.***1191** Enea has also filed a motion for summary judgment as to the Second and Third Claims of Baghai's Counterclaim against Enea. For the reasons discussed below, Enea's motion for summary judgment as to Plaintiffs' claims is **GRANTED IN PART** and **DENIED IN PART,** Counterdefendants' first motion for partial summary judgment is **GRANTED IN PART** and **DENIED IN PART,** Counterdefendants' second motion for partial summary judgment is **DENIED,** and Enea's motion for summary judgment on the Second and Third Claims of Baghai's Counterclaim is **GRANTED.**

I. *FACTUAL BACKGROUND*

This case arises out of a dispute between Enea and

two of its former employees, Hilderman and Baghai.

Hilderman was the founder of TekSci, Inc., which was sold to Enea AB in 2000. The company became known as "Enea–TekSci" or Enea. Enea is a software consulting company that provides, among other things, software, systems development, consulting and training, and software certification for critical and real-time systems such as those systems found in the avionics industry, the telecommunications industry, and the medical industry.

Hilderman continued as an employee of Enea until he left the company in February 2004. In February 2004, Hilderman and Enea entered into a Severance Agreement. (Pls.' Ex. A.) The Severance Agreement provided, among other things:

> 17. *Confidentiality*. Employee agrees to keep confidential all trade secrets, confidential, and proprietary information of Enea obtained by Employee during the course of his employment with Enea, including, but not limited to, information pertaining to product offerings, pricing and marketing structures and strategies, software programs existing or under development, and the identities of current and prospective customers, to the extent such information is not generally available to the public.
>
> 18. *Anti–Piracy and Noncompetition.* Employee shall not, for a period of six (6) months after the Resignation date, either on his own account or in conjunction with any other person, firm, or company;
>
> (a) Solicit or entice away, or attempt to solicit or entice away, from Enea or from its parent or any affiliated or subsidiary corporation, any person employed by Enea on the Resignation Date;
>
> (b) Solicit or attempt to solicit the business of any person, firm or company who has at any time within one year prior to the Resignation Date been a customer or client of Enea or its parent or any affiliated or subsidiary corporation.

The Severance Agreement provides that it shall be construed and interpreted according to the laws of the State of California. (Pls.' Ex. A at ¶ 12.)

In February 2005, Hilderman formed HighRely. HighRely, like Enea, is engaged in the business of providing engineering support and development to clients in need of embedded high-reliability software services.

HighRely employed Ray Madjidi ("Madjidi"), a former project manager for Enea, and Baghai, also a former employee of Enea. Baghai and Madjidi ceased employment at Enea in March 2005. There is a dispute as to when Baghai and Madjidi began working for HighRely. Hilderman is a shareholder of HighRely, but is not an employee.

In late March, 2005, Boeing contacted Baghai regarding work on C–17 document verification. Baghai claims that he had been fired before being contacted by Boeing.***1192** Enea disputes Baghai's claim that he had been terminated. In April, 2005 HighRely obtained a contract with Boeing.

HighRely provided services on Boeing's C–130 program throughout 2005 and part of 2006. Boeing ultimately terminated HighRely's contract, claiming that funding had ceased for the C–130 program. In March of 2005, Hilderman contacted Hospira, a medical device company, to obtain a contract for HighRely. No contract resulted from these discussions.

Hospira and Boeing were major customers of Enea during 2004 and 2005. Hilderman was involved in obtaining Hospira and Boeing as customers for Enea while he was employed at Enea. Baghai was

involved in Boeing projects while he was employed at Enea.

Plaintiffs Hilderman and HighRely claim that Enea interfered with their contract with Boeing and their prospective contract with Hospira by telling Boeing and Hospira that Hilderman was violating the terms of the Severance Agreement and was subject to a non-compete agreement. Plaintiffs assert the following causes of action: (1) declaratory relief; (2) breach of contract; (3) interference with contractual relations and prospective economic advantage; and (4) violation of California Business & Professions Code § 17200.

In its Amended Counterclaim and Third–Party Complaint, Enea claims that Baghai, while still employed by Enea, forwarded Enea's customer leads, proprietary trade secrets, employee leads, Enea employee email addresses, and other confidential information to Hilderman for the benefit of HighRely. Enea asserts causes of action for (1) breach of the duty of loyalty by Baghai; (2) misappropriation of trade secrets by Baghai, Hilderman, and HighRely, (3) aiding and abetting by Hilderman; (4) breach of contract by Hilderman and Baghai; (5) violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, by Hilderman, Baghai, and HighRely; (6) conspiracy to intentionally interfere with contract against Hilderman, Baghai, and HighRely; (7) conspiracy to intentionally interfere with prospective economic advantage against Hilderman, Baghai, and Highrely, and (8) unfair business practices, Cal. Bus. & Prof.Code § 17200, against Hilderman, Baghai, and HighRely.

In his Counterclaim, Baghai alleges that he was wrongfully terminated in breach of his employment agreement. Baghai further alleges that company policy provided that he would have the right to purchase his laptop computer upon termination, but that Enea refused to allow him to do so. According to Baghai, Enea accessed his private e-mail accounts and other information on the computer in violation of company policy. The Counterclaim asserts causes of action for (1) breach of contract; (2) intrusion into private affairs; (3) violation of the Electronic Communications Privacy Act ("ECPA") (18 U.S.C. §§ 2510–2522, 18 U.S.C. §§ 2701–2711); and (4) intentional infliction of emotional distress ("IIED"). In an order filed on June 13, 2006, the Court dismissed Baghai's claim under Title II of the ECPA (Baghai's claim under Title I survived) and IIED claim.

II. *STANDARD OF REVIEW*

[1][2][3] Summary judgment is appropriate under Rule 56 of the Federal Rules of Civil Procedure if the moving party demonstrates the absence of a genuine issue of material fact and entitlement to judgment as a matter of law. *Celotex Corp. v. Catrett*, 477 U.S. 317, 322, 106 S.Ct. 2548, 91 L.Ed.2d 265 (1986). A fact is material when, under the governing substantive law, it could affect the outcome of the case. ***1193***Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986); *Freeman v. Arpaio*, 125 F.3d 732, 735 (9th Cir.1997). A dispute is genuine if a reasonable jury could return a verdict for the nonmoving party. *Anderson*, 477 U.S. at 248, 106 S.Ct. 2505.

[4][5][6] A party seeking summary judgment always bears the initial burden of establishing the absence of a genuine issue of material fact. *Celotex*, 477 U.S. at 323, 106 S.Ct. 2548. The moving party can satisfy this burden in two ways: (1) by presenting evidence that negates an essential element of the nonmoving party's case; or (2) by demonstrating that the nonmoving party failed to establish an essential element of the nonmoving party's case on which the nonmoving party bears the burden of proving at trial. *Id.* at 322–23, 106 S.Ct. 2548. "Disputes over irrelevant or unnecessary facts will not preclude a grant of summary judgment." *T.W. Elec. Serv., Inc. v. Pacific Elec. Contractors Ass'n*, 809 F.2d 626, 630 (9th Cir.1987).

[7][8][9] Once the moving party establishes the

absence of genuine issues of material fact, the burden shifts to the nonmoving party to set forth facts showing that a genuine issue of disputed fact remains. *Celotex*, 477 U.S. at 322, 106 S.Ct. 2548. The nonmoving party cannot oppose a properly supported summary judgment motion by "rest[ing] on mere allegations or denials of his pleadings." *Anderson*, 477 U.S. at 256, 106 S.Ct. 2505. When ruling on a summary judgment motion, the court must view all inferences drawn from the underlying facts in the light most favorable to the nonmoving party. *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587, 106 S.Ct. 1348, 89 L.Ed.2d 538 (1986).

III. *DISCUSSION*

A. *Enea's Motion For Summary Judgment*

Enea moves for summary judgment on all of the claims asserted by Hilderman and HighRely. The Court will address each of the claims in turn.

1. *Declaratory Relief*

Plaintiffs seek a declaration that pursuant to the Severance Agreement, Hilderman is entitled to solicit business, customers and employees of Enea after August 13, 2004.

[10][11][12] The "actual controversy" requirement of the Declaratory Judgment Act is the same as the "case or controversy" requirement of Article III of the United States Constitution. *Aetna Life Ins. Co. v. Haworth*, 300 U.S. 227, 239–40, 57 S.Ct. 461, 81 L.Ed. 617 (1937). Article III requires that there be a "substantial controversy ... of sufficient immediacy and reality to warrant the issuance of a declaratory judgment." *Maryland Casualty Co. v. Pacific Coal & Oil Co.*, 312 U.S. 270, 272, 61 S.Ct. 510, 85 L.Ed. 826 (1941). "[A]n actual controversy must be extant at all stages of review, not merely at the time the complaint is filed." *Arizonans for Official English v. Arizona*, 520 U.S. 43, 67, 117 S.Ct. 1055, 137 L.Ed.2d 170 (1997) (internal quotation marks and citations omitted).

[13] Enea does not dispute that under the terms of the Severance Agreement, Hilderman is permitted to solicit employees and customers of Enea after August 13, 2004, *provided that* Hilderman complies with the confidentiality provision of the Severance Agreement and does not use confidential, proprietary or trade secret information of Enea. The controversy surrounds what constitutes confidential, proprietary or trade secret information that Hilderman is prohibited from using and whether Hilderman/HighRely used any such information in the pursuit of hiring employees or obtaining new business.

***1194** Plaintiffs' declaratory relief claim misframes the issue. There is no dispute that Hilderman can solicit employees and customers of Enea after the initial six-month period as long as no confidential, proprietary or trade secret information is used in the process. Because there is no actual dispute within the claim for declaratory relief, the Court grants summary judgment in favor of Enea, dismissing the claim without prejudice.

2. *Breach of Contract*

[14] Plaintiffs allege that Enea breached the terms and provisions of the Severance Agreement by falsely telling third parties that Hilderman had agreed to a non-compete clause and was breaching that agreement by soliciting former employees or customers of Enea.

Enea argues that there is no contract term which gives Hilderman the unfettered right to solicit Enea's customers and employees after six months and that Hilderman was obligated to respect Enea's confidential information. However, there are triable issues as to whether Hilderman used any confidential, proprietary or trade secret information to obtain customers or employees.

It was an implied term of the contract that Hilderman could, after six months, solicit Enea's cus-

tomers and employees provided that there was no use of confidential, proprietary, or trade secret information. *See* Cal. Civil Code § 1656 ("All things that in law or usage are considered as incidental to a contract, or as necessary to carry it into effect, are implied therefrom ....") If Enea told potential customers or employees not to deal with Hilderman/HighRely because Hilderman was in breach of a non-compete agreement, it is arguable that Enea breached the implied covenant of good faith and fair dealing by attempting to deprive Hilderman of enjoying the benefits of the agreement—i.e., the right, under certain circumstances, to solicit employees and customers of Enea. *See Guz v. Bechtel National Inc.*, 24 Cal.4th 317, 349, 100 Cal.Rptr.2d 352, 8 P.3d 1089 (2000) (explaining that the covenant of good faith and fair dealing, which is implied by law in every contract, prevents one contracting party from unfairly frustrating the other party's right to receive the benefits of the agreement actually made.).

Enea argues that Hilderman has no proof that Enea told anyone that Hilderman was subject to a non-compete agreement and could not lawfully solicit employees or customers of Enea. However, Hilderman and HighRely have raised a triable issue of material fact in this regard. In his deposition, Hilderman explained that Neal Holland of Hospira told him that Hospira did not want to do business with him because individuals at Enea (Virginia Walker and Victoria Barrett) had told Holland that Hilderman had stolen things and was violating his noncompete agreement by even talking to Hospira. (Hilderman Dep. (Pls.' Ex. L), 38:18–39:1.) Hilderman also explained that individuals from Boeing management made direct statements regarding the potential for legal problems if Boeing hired HighRely. (Hilderman Dep., 50:22–51:3.)

Enea contends that Hilderman has not suffered any damages personally from the alleged breach. Hilderman contends otherwise but does not detail exactly what damages he is claiming. This issue was not fully briefed, and it is unclear to the Court whether Hilderman can recover any damages. Therefore, the Court denies Enea's motion as to this claim without prejudice. The Court gives Enea leave to file a new motion for summary judgment limited to the issue of Hilderman's contract damages. The moving and opposition papers shall be limited to 10 pages ***1195** each, and the reply shall not exceed 5 pages. If such a motion is brought, Hilderman's opposition must specify each and every element of his claimed damages.

[15][16] Enea also challenges HighRely's standing to bring the breach of contract claim. The Court agrees that HighRely, who was not a party to the contract, lacks standing to assert this claim. HighRely argues that it is a third-party beneficiary of the contract. The Court is not persuaded by this argument. "The circumstance that a literal contract interpretation would result in a benefit to the third party is not enough to entitle that party to demand enforcement. The contracting parties must have intended to confer a benefit on the third party." *Neverkovec v. Fredericks*, 74 Cal.App.4th 337, 348, 87 Cal.Rptr.2d 856 (1999). To determine whether a third party is an intended beneficiary or merely an incidental beneficiary to the contract involves "construction of the parties' intent, gleaned from reading the contract as a whole in light of the circumstances under which it was entered." *Jones v. Aetna Cas. & Surety Co.*, 26 Cal.App.4th 1717, 1725, 33 Cal.Rptr.2d 291 (1994).

[17] Here, the Severance Agreement arose out of Hilderman's resignation from Enea and concerned the respective duties and rights of Hilderman, as a former employee and potential competitor, and Enea. At the time the parties entered into the agreement, HighRely was not yet in existence, and no mention was made in the Severance Agreement regarding any companies or corporate entities that might be formed by Hilderman in the future. Although any company formed by Hilderman would benefit from Hilderman being allowed to pursue Enea's employees and customers, there is no indication in the contract that the parties specifically

intended to confer a benefit on such a separate entity.

[18] Plaintiffs point to the following language in the Severance Agreement:

> The parties understand and expressly agree that this Agreement shall bind and *benefit* the heirs, parents, subsidiaries, partners, *successors*, employees, directors, stockholders, officers, attorneys, affiliates, predecessors, representatives and assigns of Employee and Enea. Enea specifically represents that it has the authority to bind its parent corporation to this Agreement to the extent this Agreement creates obligations of the Parent.

(Severance Agreement, ¶ 11) (emphasis added). Plaintiffs argue that HighRely is a "successor" who is entitled to enforce the benefits of the contract. However, Plaintiffs do not cite any authority for deeming a corporation a "successor" to an individual party to a contract. HighRely is not a "successor" under any ordinary meaning of the word. *See Black's Law Dictionary* (8th ed.2004) (defining successor as "one who replaces or follows a predecessor").

Accordingly, the Court denies Enea's motion for summary judgment as to Hilderman's breach of contract claim but grants the motion as to HighRely's breach of contract claim.

3. *Interference with Contract and Interference with Prospective Economic Advantage*

Relying on *Marin Tug & Barge, Inc. v. Westport Petroleum, Inc.*, 271 F.3d 825 (9th Cir.2001), Enea argues that it cannot be sued for interference with contract or prospective contract because it was not a "stranger" to Hospira and Boeing because it had preexisting relationships with them. Enea's reliance on *Marin Tug* is misplaced. In *Marin Tug*, after Marin Tug, an operator of barges, sued Shell Oil Products Company over the purchase of contaminated fuel, Shell refused to contract with the barge operator and refused to ***1196** allow its oil to be carried on the operator's barges. Marin Tug sued Shell for intentional interference with prospective economic advantage. The Ninth Circuit held that Marin Tug's claim failed because Shell did not engage in any wrongful conduct. The Ninth Circuit also noted that Shell was not a stranger to the relationship between Marin Tug and the buyer of any Shell oil shipped on Marin Tug's barges, because such relationships required direct, active involvement by Shell-the loading of Shell oil onto Marin Tug's barges. *Id.* at 834. The Ninth Circuit concluded that it was not wrongful for Shell to simply refuse to deal with Marin Tug or to load its oil on Marin Tug's barges.

[19] Here, even though Enea had its own relationships with Hospira and Boeing, it did not have any involvement in the relationship between HighRely and the companies. Enea was an outsider to HighRely's contractual relationships with the companies and can be held liable for intentionally interfering with the contracts/prospective contracts. *See Applied Equipment Corp. v. Litton Saudi Arabia Ltd.*, 7 Cal.4th 503, 513–14, 28 Cal.Rptr.2d 475, 869 P.2d 454 (1994)

[20] Enea argues that there is no evidence that HighRely lost any existing contracts as a result of Enea's alleged conduct. According to Robert Allard of Boeing, HighRely's work for Boeing came to an end about December 2005 because funding had run out at that time. (Allard Dep. (Enea's Ex. E), 78:2–9.) In a declaration, Hilderman states that he is personally aware of the C–130 program and the fact that it has continued through this date. (Hilderman Decl. ¶ 10.) Hilderman claims that much of the C–130 work has been given to Enea "who has earned literally millions of dollars in the continuation of this work all at the expense of HighRely." (*Id.*) However, Hilderman fails to establish the basis for his alleged knowledge that the C–130 program never ran out of funds and continued to the present. Hilderman has not made any showing that he has personal knowledge of these facts. Therefore, Enea is entitled to summary judgment on

the interference with contract claim.

[21][22] With respect to the interference with prospective economic advantage claim, Enea argues that there is no evidence that it wrongfully caused HighRely to lose potential business. The elements of an interference with prospective economic advantage ("IPEA") claim are: (1) an economic relationship between the plaintiff and a third party that carries a probability of future economic benefit to the plaintiff; (2) defendant's knowledge of the relationship; (3) intentional acts on the part of the defendant designed to disrupt the relationship; (4) actual disruption of the relationship; and (5) economic harm to the plaintiff proximately caused by the defendant's acts. *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal.4th 1134, 1153–54, 1164–65, 131 Cal.Rptr.2d 29, 63 P.3d 937 (2003). Furthermore, the plaintiff must allege that the defendant's act was "wrongful 'by some measure beyond the fact of the interference itself.' " *Della Penna v. Toyota Motor Sales, U.S.A., Inc.*, 11 Cal.4th 376, 392–93, 45 Cal.Rptr.2d 436, 902 P.2d 740 (1995) (quoting *Top Serv. Body Shop, Inc. v. Allstate Ins. Co.*, 283 Or. 201, 582 P.2d 1365, 1371 (1978)).

[23] Enea argues that Hilderman/HighRely did not have an existing economic relationship with Hospira. However, according to Hilderman, in or about March of 2005, he contacted Hospira to obtain a contract for HighRely. (Hilderman Decl. ¶ 12.) Hospira indicated that they had a need for further engineering talent and indicated that they would enter into an agreement for HighRely's engineering services. (*Id.*) However, Hospira later informed Hilderman that it did not ***1197** want to enter into a contract with HighRely because Enea claimed that Hilderman was in violation of a non-compete agreement. (*Id.*) This evidence raises a triable issue with respect to the existence of an economic relationship carrying a probability of future economic benefit to HighRely.

[24][25] Enea also argues that HighRely fails to satisfy the requirement of an independent wrong. An act is independently wrongful "if it is unlawful, that is, if it is proscribed by some constitutional, statutory, regulatory, common law, or other determinable legal standard." *Korea Supply*, 29 Cal.4th at 1159, 131 Cal.Rptr.2d 29, 63 P.3d 937. It is arguable that Enea's actions were independently wrongful because they breached the covenant of good faith and fair dealing that was implied in the Severance Agreement with Hilderman. [FN1] Furthermore, as discussed below, Plaintiffs' section 17200 claim survives summary judgment. A violation of section 17200 can satisfy the requirement of an independently wrongful act. *CRST Van Expedited, Inc. v. Werner Enter., Inc.*, 479 F.3d 1099, 1110 (9th Cir.2007).

FN1. Although cases have held that a defendant's breach of a contract with the plaintiff "cannot be transmuted into tort liability by claiming that the breach detrimentally affected the [plaintiff's] business," *JRS Products, Inc. v. Matsushita Electric Corp. of America*, 115 Cal.App.4th 168, 180–83, 8 Cal.Rptr.3d 840 (2004), the Court did not locate any cases dealing with situations where the independent wrong is a breach of a contract between the defendant and a third-party. As discussed *infra*, the IPEA claim belongs to HighRely.

[26] However, the IPEA claim belongs to HighRely only. The Court agrees with Enea that Hilderman lacks standing to pursue the IPEA claim, which is based on a potential contract between HighRely and Hospira. *See Sutter v. General Petroleum Corp.*, 28 Cal.2d 525, 530, 170 P.2d 898 (1946) (explaining that as a general matter, a stockholder may not maintain an action in his own behalf for a wrong done by a third person to the corporation on the theory that such wrong devalued his stock).

[27] Furthermore, HighRely has failed to raise a triable issue as to Enea's alleged interference with prospective contracts with Boeing. As discussed

above, Hilderman has not shown that he has personal knowledge regarding the continuation of the C–130 program. Therefore, there is no evidence from which to infer that Boeing ceased doing business with HighRely as a result of Enea's actions and that HighRely lost contracts that it would otherwise have been awarded.

In sum, the Court grants Enea's motion for summary judgment as to Hilderman's and HighRely's intentional interference with contract claim, Hilderman's IPEA claim, and HighRely's IPEA claim to the extent it is based on the loss of prospective contracts with Boeing. The Court denies' Enea's motion as to HighRely's IPEA claim with respect to the loss of a prospective contract with Hospira.

4. *Section 17200 Claim*

[28] Enea argues that summary judgment should be granted on Plaintiffs' section 17200 claim because there is no evidence that Enea is falsely claiming to businesses and customers that Hilderman is the subject of a covenant not to compete. However, as discussed above, Hilderman claims that Neal Holland of Hospira told him that Virginia Walker and Victoria Barrett stated that Hilderman had stolen things and was violating the non-compete agreement by talking to Hospira. (Hilderman Dep. 38:18–25.) Therefore, Enea's motion for summary judgment is denied on this claim.[FN2]

FN2. In their opposition, Hilderman and HighRely argue that Enea also violated section 17200 by (1) attempting to enforce an unenforceable non-compete clause in a 2003 employment contract with Baghai; and (2) using photographs of Baghai and Madjidi in an Enea product catalog without obtaining their permission. These claims exceed the scope of the complaint, which alleges only that Enea violated section 17200 by falsely claiming that Hilderman was the subject of a covenant not to compete.

***1198** B. *Counterdefendants' Motions for Partial Summary Judgment*

In their first motion, Counterdefendants move for summary judgment on Enea's misappropriation of trade secret claim to the extent it is based on (1) the alleged misappropriation of DO–178B checklists and processes; and (2) the alleged misappropriation of trade secrets in connection with entering into a contract with Boeing. For the reasons discussed below, the Court grants Counterdefendants' motion with respect to the DO–178B checklists and processes and denies the motion with respect to the Boeing contract.

In their second motion, Counterdefendants seek summary judgment that (1) there is no trade secret with respect to Enea's customers, customer contact information, and customer pricing; (2) Enea's employees were not trade secrets and were not wrongfully solicited by Counterdefendants; and (3) Baghai's operative employment agreement with Enea did not contain a non-solicitation provision. The Court denies this motion.

1. *DO–178 B Checklists & Processes*

[29] The FAA requires that all avionics software meet testing and certification standards set forth in DO–178B, a published regulation. (Hilderman Decl. ¶ 8.) In the late 1990's Hilderman and Baghai wrote TekSci's DO–178B processes and checklists. Enea claims that these DO–178B processes and checklists are trade secrets that were misappropriated by Counterdefendants.

California's Uniform Trade Secrets Act defines a trade secret as follows:

> "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
>
> (1) Derives independent economic value, actual

> or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and
>
> (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.
>
> Cal. Civ.Code § 3426.1(d).

Counterdefendants contend that Enea's DO–178B processes and checklists were based on a variety of public domain sources and do not contain any unique information that derives economic value from being kept secret. Hilderman and Baghai explain that the processes and checklists were prepared from public domain sources including the regulation itself and checklists prepared by Boeing ("D6 checklists"). (Hilderman Decl. ¶¶ 11, 13; Baghai Decl. ¶ 9.) The "vast majority" of the information reflected in Enea's DO–178B processes and checklists was taken from the D6 checklists, which were publicly available. (Hilderman Decl. ¶ 13.)

Enea does not explain how its DO–178B processes and checklists are different from or an improvement upon the information that is publicly available. Connie Beane of Enea states that Boeing's D6 checklists consist of a total of 22 checklists, whereas Enea has 133 checklists. (Beane Decl. ¶ 13.) However, Enea still fails to present any evidence that its checklists set forth information that is not generally known within the industry. Victoria Barrett, the individual designated by Enea under Fed.R.Civ.P. 30(b)(6) to testify regarding the trade secret claims, could not explain what sets Enea's checklists apart from other ***1199** publicly available checklists other than that she heard Enea's checklists "track" DO–178B better. (Barrett Dep. (HighRely Ex. G), 125:15–126:25.)

[30] Enea argues that Counterdefendants are estopped from arguing that the DO–178B processes and checklists are trade secrets. Enea's estoppel argument fails for several reasons. First and foremost, the doctrine of estoppel requires, among other things, that the party invoking the doctrine have relied upon the statement or conduct at issue to his injury. *DRG/Beverly Hills, Ltd. v. Chopstix Dim Sum Cafe and Takeout III, Ltd.*, 30 Cal.App.4th 54, 59, 35 Cal.Rptr.2d 515 (1994); Cal. Evid.Code § 623. Even if Counterdefendants made prior representations that the DO–178B processes and checklists were trade secrets, Enea has not shown how it relied upon these representations to its detriment. No trade secrets were valued in the sale of TekSci to Enea. (Hubbard Decl. ¶ 4.) TekSci's valuation was based strictly on its earnings and a multiplier of the earnings. (Hubbard Decl. ¶ 3.)

[31] Moreover, the prior statements upon which Enea relies are, for the most part, vague puffery or references to "proprietary" information, which is not the same thing as trade secrets. For example, Hilderman's statement that TekSci "invested over one million dollars in our technical and management processes and they are very unique" does not detail what is unique about the processes, which, at any rate, presumably include more than the DO–178B processes and checklists. (Enea Ex. 6.) Marketing materials and other documents authored by Hilderman and/or Baghai refer to the DO–178B processes and checklists as "proprietary." (Enea Exs. 5, 9, 14, 15, 18, 20, 32, 56.) However, the processes and checklists were apparently copyrighted. A proprietary interest in a copyright or other intellectual property does not necessarily constitute a trade secret. *See Buffets, Inc. v. Klinke*, 73 F.3d 965, 968 (9th Cir.1996) (explaining the difference between copyright, which protects a particular expression of an idea, and trade secret law, which protects an author's very ideas).

[32] Enea also attempts to invoke the doctrine of judicial estoppel, arguing that Hilderman took a contrary position in a copyright infringement/misappropriation of trade secret action brought

against Enea by ELDEC. In response, Hilderman has submitted documents filed in that action, which show that TekSci/Hilderman actually defended the suit by arguing that the structural coverage document at issue was based upon publicly available information and was *not* a trade secret. (HighRely Exs. D, E.) Based on the documents before the Court, Hilderman did not take an inconsistent position during the ELDEC litigation and is not judicially estopped.

[33] Enea has failed to raise a triable issue of material fact with respect to whether its DO–178B checklists and processes derive independent economic value from not being generally known to the avionics industry. Therefore, the Court grants summary judgment on Enea's trade secret claim to the extent it is based on the DO–178B checklists and processes. The Court does not reach the issues of whether Enea took reasonable efforts to maintain the secrecy of the DO–178B checklists and processes or whether HighRely uses or has used the checklists and process.[FN3]

> FN3. In its opposition papers, Enea claims that Counterdefendants have hidden and destroyed evidence. Enea requests that the Court issue an order that Counterdefendants' destruction of evidence and failure to produce is a violation of the law. Enea also requests that the Court instruct the jury that they can infer that Counterdefendants stole trade secrets, profited from them, and have concealed the conduct. If Enea believed that Counterdefendants engaged in discovery abuse, Enea should have raised the issue before the Magistrate Judge. Counterdefendants' conduct during discovery is not properly before the Court at this time.

***1200** 2. *Boeing Contract*

[34] Enea contends that Counterdefendants stole the Boeing account and misappropriated trade secrets in the process. Although Enea concedes that the identity of Boeing was not a trade secret, Enea contends that the contact information regarding Robert Allard at Boeing was a trade secret. In addition, Enea argues that a jury could find that HighRely used Enea's pricing information to bid on the Boeing project at a lower price and take the business from Enea.

Enea has not established that the contact information of Robert Allard was a trade secret. According to Baghai, he was introduced to Allard in or about 1996, while he was at TekSci, and has had a long-standing professional relationship with him. (Baghai Decl. in Support of Reply ¶ 3.) Baghai also explains that Boeing frequently directs outside suppliers to Allard and provides them with his contact information. Enea has not provided any evidence to the contrary. Therefore, there is no basis for finding that Allard's contact information was a trade secret. *See AdvantaCare Health Partners, L.P. v. Access IV, Inc.*, 2003 WL 23883596 (N.D.Cal. Oct.24, 2003) (explaining that referral sources solicited by Defendants were known in the industry—"Any newcomer to the industry would be able to discover the identities of these sources and to solicit them.").

[35] However, there is a triable issue of material fact with respect to Enea's pricing information. Counterdefendants argue that Enea's pricing was not a trade secret because Enea priced its engineers at hourly rates that reflect market rates known to the industry. (Baghai Decl. ¶ 5; Walonoski Dep. (Enea Ex. B in Support of Reply), 70:18–71:8.) Although Enea's prices may have generally reflected market rates, Enea has presented evidence that Enea uses different price lists for different customers. (Elliot Decl. in support of Enea's opp. to second motion ("Elliot Decl. 2"), ¶ 17; Elliot Dep. (Enea's Ex. 53 in opp. to second motion), 81:14–82:12.) Hilderman, while at Enea, devised a method whereby different rate sheets were linked to different suite numbers in the Enea address. (*Id.*) Only Enea knew the rate differences. (Elliot Decl. 2, ¶ 17.) This specific information regarding pricing differences among Enea's various customers arguably would derive independent

economic value from not being generally known to the public. Thus, the Court denies summary judgment on this issue.[FN4]

> FN4. The Court does not have enough information to determine whether Enea made reasonable efforts to keep the different rates secret. Enea admittedly provided rate sheets to some prospective and existing customers. (Elliot Depo. (Ex. 53), 82:4–9.) What steps Enea took to preserve the alleged secrecy of this information vis-à-vis prospective and existing customers, in addition to Enea employees, is a matter that should be addressed at trial.

[36] To the extent Enea claims that the information regarding Boeing's C–17 project was a trade secret, there is no evidence that Counterdefendants misappropriated it. Allard thought Baghai was still at Enea when he called him in March, 2005. (Allard Depo. (Enea Ex. 43–162 in opp. to second motion) 94:16–18.). However, Allard's primary purpose was to talk to Baghai in particular. The critical design review for the C17 project had already failed twice, and the Air Force specifically recommended Baghai and Hilderman. (Allard Depo. (HighRely Ex. H), 47:2–4.) Whether Baghai was fired or resigned, there is no indication that Allard's interest ***1201** in talking to Baghai about the project depended on Baghai being employed at Enea. Moreover, it appears that Allard was going to contact Hilderman/HighRely anyway. Therefore, there was no misappropriation of trade secret information regarding the C–17 project. Whether Baghai breached his duty of loyalty or any contractual provisions in the course of pursuing the Boeing project for HighRely is a separate matter that does not bear upon the trade secret claim.

3. *Enea's Customer Information*

[37] Counterdefendants claim that there is nothing secret about Enea's customers. According to Counterdefendants, these avionics customers are readily ascertainable. Enea counters that the identity of its customers and projects is not published or known generally and that Enea has spent money developing the customer list through its marketing programs. (Elliot Decl. 2 ¶ ¶ 8–9.)

[38][39][40] Client lists can receive trade secret protection if they satisfy the requirements of Cal. Civ.Code § 3426.1(d). *Reeves v. Hanlon*, 33 Cal.4th 1140, 1155, 17 Cal.Rptr.3d 289, 95 P.3d 513 (2004) As explained in *Morlife, Inc. v. Perry*, 56 Cal.App.4th 1514, 1521–22, 66 Cal.Rptr.2d 731 (1997), where the employer has "expended time and effort identifying customers with particular needs or characteristics, courts will prohibit former employees from using this information to capture a share of the market.... [A] customer list can be found to have economic value because its disclosure would allow a competitor to direct its sales efforts to those customers who have already shown a willingness to use a unique type of service or product as opposed to a list of people who only might be interested." *See also MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 521 (9th Cir.1993) (holding that a customer database had potential economic value because it allowed competitors to direct its sales efforts to those potential customers that are already using the MAI computer system.)

Although Enea's clients may be businesses that are well-known in the avionics industry, it is unclear whether it is generally known that these particular business use the services provided by Enea. If all or almost all businesses in the avionics industry use these types of services or if the number of businesses in the avionics industry is very small then the identity of Enea's avionics clients may not qualify as a trade secret. However, Counterdefendants have not presented evidence in this regard. Therefore, there is a triable issue as to whether Enea's client list derives economic value from not being generally known to the public.

[41] Counterdefendants argue that Enea did not

make reasonable efforts to keep its client list secret because it only had confidentiality agreements with select customers and employees. Even if this is true, the lack of confidentiality agreements is not dispositive on the issue of secrecy. Enea may have taken other precautions to keep its information secret, such as verbally telling its clients and employees that the information was confidential or limiting access to information on a "need to know" basis. *See, e.g., Religious Technology Center v. Netcom On–Line Communication Services, Inc.*, 923 F.Supp. 1231, 1253 (N.D.Cal.1995). Enea claims that it takes steps to keep the information secret (Elliot Decl. 2, ¶ 9) but does not describe exactly what steps it takes. Accordingly, the Court does not have sufficient information to determine whether Enea took reasonable steps to keep the client list secret and will allow the claim to proceed to trial.

As for Enea's pricing information, as discussed above, there is a triable issue with respect to whether the different rate ***1202** sheets used by Enea qualify as a trade secret. Thus, Counterdefendants' motion for summary judgment is denied with respect to Enea's pricing and customer information.

4. *Enea's Employees and Engineers*

[42] Counterdefendants argue that there is no evidence of any use of trade secrets in connection with the solicitation of Enea's engineers. Counterdefendants point out that the majority of the employees hired by HighRely were independent contractors and did not work at Enea at the time they joined HighRely. Even if this is so, there is still a triable issue regarding the misappropriation of trade secrets in connection with the solicitation for Enea's engineers.

According to Enea, engineers are recruited by paid recruiters. (Elliot Decl. 2, ¶ 8.) The employee and engineer list was on a server at Enea protected by a password. (Elliot Decl. 2, ¶ 9.) The engineer list had limited access. (*Id.*) Baghai had access to the engineer contact list. (*Id.*) On March 16, 2005, Baghai forwarded to Hilderman an e-mail contact list for Enea's employees and contractors. That same day, Hilderman sent an e-mail to Enea's employees and engineers, urging them to think about various issues before signing a confidentiality agreement with Enea. (Enea's Ex. 30 in opp. to second motion.) In addition to discussing the validity/invalidity of non-compete agreements, the e-mail discussed the formation of HighRely:

> Yes, I am starting a new company. There has never been any secret to that. Please note that we fully intend to hire the best engineers and personnel available, subject to their availability, interest, and presenting a strong win/win situation. In other words, the same recipe for success we employed 15 years ago when we created what became the largest and best real-time consulting company in the West. Our new company has far greater plans than that however, and those will be announced via the grand opening of our new headquarters building in Phoenix; recently purchased and being completed now our operations will begin in May 2005 and key employees are already coming on-board; financing and partnerships are completed also.

The e-mail also explained, "Your non-compete does not restrict you from speaking to me about job opportunities, whether you call me or I call you." It appears that Ali Motamedi, Brad Dubois, and Jimmy Terry, all of whom subsequently joined HighRely, received this e-mail. (Enea's Ex. 21 in opp. to second motion.) This evidence raises a triable issue as to whether Counterdefendants used trade secret information to solicit employees for HighRely. Whether Enea can prove damages resulting from the misappropriation of the employee/contractor contact list is a separate issue to be resolved at trial.

The Court rejects Counterdefendants' argument that because, under the Severance Agreement, Hilderman was allowed to solicit Enea's employees after 6 months, any trade secret protection with respect to

employee information was waived. It seems that it would be possible for Hilderman to solicit employees without misappropriating trade secrets—e.g., Hilderman could contact employees or contractors he knew while he was at Enea by independently obtaining telephone numbers or e-mail addresses.

5. *Baghai's Employment Agreement*

Baghai contends that his 2003 employment agreement (Enea Ex. 3 in opp. to second motion), which contains a non-solicitation provision, was superceded by a July 28, 2004 employment agreement (HighRely's Ex. E–2 in support of second motion), which does not contain a non-solicitation clause. Enea disputes the validity of the ***1203** unsigned July 28, 2004 employment agreement.

The Court declines to rule on this issue at this time. What employment agreement is the operative one does not dispose of any discrete portion of Enea's trade secret claim, nor does it eliminate Enea's breach of contract claim due to the fact that the 2004 agreement includes a confidentiality provision.

C. *Enea's Motion on Baghai's Second and Third Claims*

Enea moves for summary judgment on Baghai's second cause of action for invasion of privacy and third cause of action for violation of the Stored Communications Act, 18 U.S.C. § 2701(a)(1). The Court grants Enea's motion on both causes of action.

1. *Invasion of Privacy*

[43] The laptop computer at issue was purchased for Baghai's use by Enea. (Elliot Decl. ¶¶ 10–11.) There is a dispute as to whether Enea had a policy in place which allowed employees to purchase their laptops upon leaving the company. Baghai claims that in reliance on the policy, he used the laptop for personal purposes such as on-line banking and calendaring. (Baghai Decl. ¶ 3.) Baghai maintained a personal e-mail account at AT & T.com, which was used for personal and private e-mails. (*Id.* at ¶ 5.) He accessed the e-mail account from his laptop, and his personal log-in and password were stored on the computer. (*Id.*) Baghai saved some of his e-mails on his computer's hard drive. (*Id.* at ¶ 6.) When Baghai left Enea, he attempted to exercise the option to purchase the laptop but was refused. (*Id.* at ¶ 4.) Baghai told Enea that he did not consent to them accessing any of the information on the computer. (*Id.*)

Enea denies that the policy allowing employees to purchase company laptop computers was still in effect. Enea explains that after it discovered Hilderman's mass e-mail to Enea employees regarding the confidentiality agreement, Enea inspected the laptop to determine whether Baghai was providing confidential information to Hilderman. (Elliot Decl. ¶ 12.) Charles Elliot, Controller of Enea, explains that to his knowledge, he is the only Enea employee who accessed the computer. (*Id.* at ¶ 14.) Elliot states that he did not look for or find any intimate information, pictures, or data of Baghai's on the laptop. (*Id.* at ¶ 15.) He also states that Enea has not accessed Baghai's AT & T e-mail account, although it has accessed e-mails saved to the computer. (*Id.* at ¶ 17.)

[44][45][46] Under Arizona and California law, the elements for invasion of privacy are: (1) an intentional intrusion into a private place, conversation, or matter (2) in a manner highly offensive to a reasonable person. *Shulman v. Group W Productions, Inc.*, 18 Cal.4th 200, 231, 74 Cal.Rptr.2d 843, 955 P.2d 469 (1998); *Medical Lab. Mgmt. Consultants v. American Broadcasting Companies, Inc.*, 306 F.3d 806, 812 (9th Cir.2002). To prevail on the first element, the plaintiff must show that he had a reasonable expectation of seclusion or solitude in the place, conversation, or data source. *Medical Lab.*, 306 F.3d at 812–13. In determining whether an alleged intrusion is "highly offensive" for purposes of the second element, relevant considerations include "the degree of the intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objec-

tives, the setting into which he intrudes, and the expectations of those whose privacy is invaded." *Id.* at 819 (quoting *Deteresa v. Am. Broad. Cos.*, 121 F.3d 460, 465 (9th Cir.1997)).

There is a triable issue as to whether Baghai has satisfied the first element. Although Elliot denies finding any intimate ***1204** information, it seems that in the process of searching for pertinent information, Elliot would have inevitably stumbled upon some of the personal information stored on the computer. Whether Baghai had a reasonable expectation of privacy in the personal data saved on the computer depends on whether Enea still had a policy of allowing employees to purchase their laptops. There is a genuine issue of material fact in this regard.

However, the Court finds as a matter of law that Enea's purported intrusion into Baghai's personal matters was not "highly offensive." Although Baghai might have believed that he could purchase the computer upon leaving the company, the computer was, until that time, Enea's property. Enea did not look at the computer for the purpose of rooting out personal information about Baghai, but, rather, was motivated by a desire to protect its confidential information and to ensure that Baghai was not engaged in unauthorized activity that would harm Enea. Although Elliot may have come across some personal information while searching the computer, there is no evidence that Elliot used the laptop to access Baghai's AT & T e-mail account or otherwise pry into Baghai's personal affairs. In addition, the intrusion was limited to Elliot himself and perhaps a forensic computer specialist. (Elliot states that the laptop was sent to a forensic computer specialist for "safe keeping.") (Elliot Decl. ¶ 14.) The laptop was not passed around the company, but, rather, was kept in Elliot's locked office until it was sent to the forensic computer specialist. (*Id.*)

The facts of this case are distinguishable from cases where a defendant hacks into someone's home computer for purposes of finding out personal information. Considering all of the circumstances, the Court concludes that the alleged invasion of privacy was not "highly offensive." Therefore, the Court grants summary judgment in favor of Enea on this cause of action.

2. *Stored Communications Act*

Previously, the Court denied Enea's motion to dismiss Baghai's claim that Enea violated 18 U.S.C. § 2701(a)(1) because Baghai alleged that Enea accessed his e-mail communications which were stored on his e-mail provider's server.

[47] Baghai has not presented any evidence that Enea accessed his e-mail account and read e-mails stored on the AT & T server. Although Enea accessed e-mail messages stored on the *laptop computer*, these actions do not violate section 2701(a)(1).

Section 2701(a) provides:

> Offense.—Except as provided in subsection (c) of this section whoever—
>
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

It is questionable whether the laptop computer qualifies as a "facility through which an electronic communication service is provided.' " *See Theofel v. Farey–Jones*, 359 F.3d 1066, 1077 n. 4 (9th Cir.2004) (noting Defendants' argument that Plaintiffs' computers are not "facilities" covered by section 2701(a)(1)). However, even setting this issue aside, the e-mail

messages stored on the hard drive do not constitute "electronic storage" within the meaning of the Stored Communications Act. The Act defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission ***1205** thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). Because subsection (A) applies only to messages in "temporary, intermediate storage," courts have construed subsection (A) as applying to e-mail messages stored on an ISP's server pending delivery to the recipient, but not e-mail messages remaining on an ISP's server after delivery. *See Theofel*, 359 F.3d at 1075. E-mails stored on the laptop computer are not in "temporary, intermediate storage." Furthermore, the e-mails on the laptop are not stored "by an electronic communication service for purposes of backup protection" as required by subsection (B).

The e-mails stored on the computer are not in "electronic storage" as defined by the Stored Communications Act. Therefore, Enea is entitled to summary judgment on this claim.

IV. *CONCLUSION*

For the reasons discussed above, Enea's motion for summary judgment on Plaintiff's Complaint [71] is **GRANTED IN PART** and **DENIED IN PART.** The motion is **GRANTED** as to Plaintiffs' declaratory relief claim, HighRely's breach of contract claim, Plaintiffs' intentional interference with contract claim, Hilderman's IPEA claim, and HighRely's IPEA claim to the extent it is based on the loss of prospective contracts with Boeing. The motion is **DENIED** as to the remaining claims.

Counterdefendants' first motion for partial summary judgment [70] is **GRANTED IN PART** and **DENIED IN PART.** The motion is **GRANTED** to the extent Enea's misappropriation of trade secret claim is based on Enea's DO–178B processes and checklists. The motion is **DENIED** with respect to Enea's claim that Counterdefendants misappropriated trade secrets, specifically pricing information, in connection with their efforts to obtain the Boeing contract. Plaintiffs have made evidentiary objections to Defendant's submissions. The Court finds these objections to be moot because the result ordered herein would be the same even if all of the objections were sustained. Therefore, it is unnecessary to rule on the objections, and they are overruled as moot.

Counterdefendants' second motion for partial summary judgment [79] is **DENIED.**

Enea's motion for summary judgment on Baghai's Second and Third Claims [78] is **GRANTED.**

IT IS SO ORDERED.

S.D.Cal.,2008.
Hilderman v. Enea TekSci, Inc.
551 F.Supp.2d 1183, 27 IER Cases 657

END OF DOCUMENT

835 F.Supp.2d 762, 33 IER Cases 442
(Cite as: 835 F.Supp.2d 762)

H

United States District Court,
N.D. California.
Jane DOE and Anne Raskin, Plaintiffs,
v.
CITY AND COUNTY OF SAN FRANCISCO, et al., Defendants.

No. C10–04700 TEH.
Dec. 13, 2011.

Background: Female employees brought action against city, county, and supervisors, alleging violations of the Federal Stored Communications Act (FSCA), California's whistleblower statutes, invasion of privacy, and intentional infliction of emotional distress, as well as several California Fair Employment and Housing Act (FEHA) violations relating to gender-based discrimination, sexual harassment, and retaliatory conduct. City and county filed motion for summary judgment.

Holdings: The District Court, Thelton E. Henderson, J., held that:
(1) genuine issue of material fact existed as to whether supervisor accessed employee's personal e-mail inbox without authorization;
(2) genuine issue of material fact existed as to whether employee had a reasonable expectation of privacy under California law in her personal e-mail while at work;
(3) genuine issue of material fact existed as to whether female employees were subject to misconduct because of their gender;
(4) genuine issue of material fact existed as to whether female employees were subjected to sexual harassment;
(5) genuine issue of material fact existed as to whether employees were subject to bullying and abuse after threatening to expose policy violations; and
(6) genuine issue of material fact existed as to whether employees were subject to extreme and outrageous conduct.

Motion granted in part and denied in part.

West Headnotes

[1] Federal Civil Procedure 170A 2519

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2519 k. Wiretapping and electronic surveillance, cases involving. Most Cited Cases

Genuine issue of material fact existed as to whether supervisor accessed employee's personal e-mail inbox without authorization, precluding summary judgment in employee's claims under the Federal Stored Communications Act (FSCA). 18 U.S.C.A. § 2701.

[2] Constitutional Law 92 1210

92 Constitutional Law
92XI Right to Privacy
92XI(A) In General
92k1210 k. In general. Most Cited Cases

Constitutional Law 92 1215

92 Constitutional Law
92XI Right to Privacy
92XI(A) In General

92k1215 k. Reasonable, justifiable, or legitimate expectation. Most Cited Cases

Torts 379 330

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)1 Privacy in General
379k330 k. In general. Most Cited Cases

To establish a claim of violation of privacy under the California Constitution, a plaintiff must show that defendants engaged in conduct which invaded plaintiff's privacy interest, that plaintiff had a reasonable expectation of privacy as to the interests invaded, that the invasion was serious, and that the invasion caused plaintiff to suffer injury, damage, loss, or harm.West's Ann.Cal. Const. Art. 1, § 1.

[3] Constitutional Law 92 1212

92 Constitutional Law
92XI Right to Privacy
92XI(A) In General
92k1212 k. Disclosure of personal matters. Most Cited Cases

Constitutional Law 92 1213

92 Constitutional Law
92XI Right to Privacy
92XI(A) In General
92k1213 k. Making of personal decisions. Most Cited Cases

Torts 379 331

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)1 Privacy in General
379k331 k. Nature and extent of right in general. Most Cited Cases

There are two recognized types of privacy interests under the California Constitution: (1) informational privacy, which is the interest in precluding dissemination or misuse of sensitive or confidential information; and (2) autonomy privacy, which is the interest in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference. West's Ann.Cal. Const. Art. 1, § 1.

[4] Constitutional Law 92 1253

92 Constitutional Law
92XI Right to Privacy
92XI(B) Particular Issues and Applications
92k1252 Public Employees and Officials
92k1253 k. In general. Most Cited Cases

Torts 379 332

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)1 Privacy in General
379k332 k. Particular cases in general. Most Cited Cases

For purposes of an invasion of privacy claim under the California Constitution, a public employee does not have a diminished expectation of privacy in his or her personal information. West's Ann.Cal. Const. Art. 1, § 1.

[5] Constitutional Law 92 1215

92 Constitutional Law
92XI Right to Privacy

92XI(A) In General
92k1215 k. Reasonable, justifiable, or legitimate expectation. Most Cited Cases

Torts 379 331

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)1 Privacy in General
379k331 k. Nature and extent of right in general. Most Cited Cases

For purposes of an invasion of privacy claim under the California Constitution, a reasonable expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms. West's Ann.Cal. Const. Art. 1, § 1.

[6] Constitutional Law 92 1253

92 Constitutional Law
92XI Right to Privacy
92XI(B) Particular Issues and Applications
92k1252 Public Employees and Officials
92k1253 k. In general. Most Cited Cases

Torts 379 332

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)1 Privacy in General
379k332 k. Particular cases in general. Most Cited Cases

For purposes of an invasion of privacy claim under the California Constitution, public employees possess some reasonable expectation of privacy in data stored on work computers, but the use of computers in the employment context carries with it social norms that effectively diminish the employee's reasonable expectation of privacy with regard to the use of his employer's computers. West's Ann.Cal. Const. Art. 1, § 1.

[7] Constitutional Law 92 963

92 Constitutional Law
92VI Enforcement of Constitutional Provisions
92VI(C) Determination of Constitutional Questions
92VI(C)1 In General
92k963 k. Questions of law or fact. Most Cited Cases

Torts 379 375

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)5 Questions of Law or Fact
379k375 k. In general. Most Cited Cases

For purposes of an invasion of privacy claim under the California Constitution, whether a legally recognized privacy interest exists is a question of law, and whether the circumstances give rise to a reasonable expectation of privacy and a serious invasion thereof are mixed questions of law and fact; if the undisputed material facts show no reasonable expectation of privacy or an insubstantial impact on privacy interests, the question of invasion may be adjudicated as a matter of law. West's Ann.Cal. Const. Art. 1, § 1.

[8] Federal Civil Procedure 170A 2515

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2515 k. Tort cases in general. Most Cited Cases

Genuine issue of material fact existed as to whether employee had a reasonable expectation of privacy in her personal e-mail while at work, precluding summary judgment in her claim of invasion of privacy in violation of the California Constitution. West's Ann.Cal. Const. Art. 1, § 1.

[9] Civil Rights 78 1166

78 Civil Rights
78II Employment Practices
78k1164 Sex Discrimination in General
78k1166 k. Practices prohibited or required in general; elements. Most Cited Cases

Civil Rights 78 1185

78 Civil Rights
78II Employment Practices
78k1181 Sexual Harassment; Work Environment
78k1185 k. Hostile environment; severity, pervasiveness, and frequency. Most Cited Cases

In order to prevail on a claim of gender discrimination under California's Fair Employment and Housing Act (FEHA), plaintiffs must prove that their managers acted with an intent to unlawfully discriminate against or harass them on the basis of their gender and that they suffered adverse employment action or, otherwise, that the alleged conduct was sufficiently severe and pervasive to alter the terms and conditions of their employment and create an abusive environment. West's Ann.Cal.Gov.Code § 12900 et seq.

[10] Civil Rights 78 1166

78 Civil Rights
78II Employment Practices
78k1164 Sex Discrimination in General
78k1166 k. Practices prohibited or required in general; elements. Most Cited Cases

The critical issue in gender claims under California's Fair Employment and Housing Act (FEHA) is whether members of one sex are exposed to disadvantageous terms or conditions of employment to which members of the other sex are not exposed. West's Ann.Cal.Gov.Code § 12900 et seq.

[11] Civil Rights 78 1118

78 Civil Rights
78II Employment Practices
78k1118 k. Practices prohibited or required in general; elements. Most Cited Cases

Civil Rights 78 1744

78 Civil Rights
78V State and Local Remedies
78k1742 Evidence
78k1744 k. Employment practices. Most Cited Cases

To establish a claim under California's Fair Employment and Housing Act (FEHA), a plaintiff must first show a prima facie case of discrimination; the plaintiff's burden is not onerous but must at least show actions taken by the employer from which one can infer, if such actions remained unexplained, that it is more likely than not that such actions were based on a prohibited discriminatory criterion. West's Ann.Cal.Gov.Code § 12900 et seq.

[12] Civil Rights 78 1744

78 Civil Rights
78V State and Local Remedies
78k1742 Evidence

78k1744 k. Employment practices. Most Cited Cases

Once a plaintiff establishes a prima facie case of discrimination for a claim under California's Fair Employment and Housing Act (FEHA), a presumption of discrimination arises; this presumption, though rebuttable, is legally mandatory and the ultimate burden of persuasion on the issue of actual discrimination remains with the plaintiff. West's Ann.Cal.Gov.Code § 12900 et seq.

[13] Civil Rights 78 1744

78 Civil Rights
78V State and Local Remedies
78k1742 Evidence
78k1744 k. Employment practices. Most Cited Cases

For purposes of a claim under California's Fair Employment and Housing Act (FEHA), whether an employer's action was motivated by actual discrimination may be proved circumstantially, from facts that create a reasonable likelihood of bias and are not satisfactorily explained. West's Ann.Cal.Gov.Code § 12900 et seq.

[14] Civil Rights 78 1118

78 Civil Rights
78II Employment Practices
78k1118 k. Practices prohibited or required in general; elements. Most Cited Cases

Civil Rights 78 1137

78 Civil Rights
78II Employment Practices
78k1137 k. Motive or intent; pretext. Most Cited Cases

For purposes of a claim under California's Fair Employment and Housing Act (FEHA), discriminatory animus need not be the sole motivation behind a challenged action; a plaintiff need only prove a causal connection between the employee's protected status and adverse employment decision. West's Ann.Cal.Gov.Code § 12900 et seq.

[15] Federal Civil Procedure 170A 2497.1

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2497 Employees and Employment Discrimination, Actions Involving
170Ak2497.1 k. In general. Most Cited Cases

Genuine issue of material fact existed as to whether female employees were subject to misconduct, including bullying by supervisors, because of their gender, precluding summary judgment in their claims of discrimination in violation of California's Fair Employment and Housing Act (FEHA). West's Ann.Cal.Gov.Code § 12900 et seq.

[16] Civil Rights 78 1036

78 Civil Rights
78I Rights Protected and Discrimination Prohibited in General
78k1030 Acts or Conduct Causing Deprivation
78k1036 k. Threats, intimidation, and harassment. Most Cited Cases

The laws prohibiting gender harassment are not intended as a general civility code.

[17] Civil Rights 78 1185

78 Civil Rights
78II Employment Practices
78k1181 Sexual Harassment; Work Environment
78k1185 k. Hostile environment; severity, pervasiveness, and frequency. Most Cited Cases

Sporadic use of abusive language, gender-related jokes, occasional teasing, or isolated or trivial comments are not enough to establish a claim of gender harassment under California's Fair Employment and Housing Act (FEHA); rather, an employee must show a concerted pattern of harassment of a repeated, routine or a generalized nature. West's Ann.Cal.Gov.Code § 12900 et seq.

[18] Civil Rights 78 1185

78 Civil Rights
78II Employment Practices
78k1181 Sexual Harassment; Work Environment
78k1185 k. Hostile environment; severity, pervasiveness, and frequency. Most Cited Cases

Gender harassment must create a hostile environment for a claim under California's Fair Employment and Housing Act (FEHA), which requires a showing of harassment sufficient that a reasonable person would consider it severe enough to alter the conditions of her employment or create an abusive working environment; whether or not such a hostile work environment exists is to be determined only by considering all the circumstances involved. West's Ann.Cal.Gov.Code § 12900 et seq.

[19] Civil Rights 78 1036

78 Civil Rights
78I Rights Protected and Discrimination Prohibited in General
78k1030 Acts or Conduct Causing Deprivation
78k1036 k. Threats, intimidation, and harassment. Most Cited Cases

Sexual harassment need not be sexual in nature to violate California's Fair Employment and Housing Act (FEHA); sexual favoritism may also constitute sexual harassment. West's Ann.Cal.Gov.Code § 12900 et seq.

[20] Federal Civil Procedure 170A 2497.1

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2497 Employees and Employment Discrimination, Actions Involving
170Ak2497.1 k. In general. Most Cited Cases

Genuine issue of material fact existed as to whether female employees were subjected to sexual harassment, precluding summary judgment in their claims under California's Fair Employment and Housing Act (FEHA). West's Ann.Cal.Gov.Code § 12900 et seq.

[21] Federal Civil Procedure 170A 2497.1

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2497 Employees and Employment Discrimination, Actions Involving
170Ak2497.1 k. In general. Most Cited Cases

Genuine issue of material fact existed as to whether city and county, who employed female employees, failed to prevent discrimination and harass-

ment of female employees from occurring, precluding summary judgment in employee's failure to prevent claims under California's Fair Employment and Housing Act (FEHA). West's Ann.Cal.Gov.Code § 12900 et seq.

[22] Civil Rights 78 1243

78 Civil Rights
78II Employment Practices
78k1241 Retaliation for Exercise of Rights
78k1243 k. Practices prohibited or required in general; elements. Most Cited Cases

A prima facie case of unlawful retaliation in violation of California's Fair Employment and Housing Act (FEHA) may be made by showing that: (1) plaintiffs engaged in activities protected by FEHA; (2) their employers subsequently took adverse employment action against them; and (3) there was a causal connection between the protected activity and the adverse employment action. West's Ann.Cal.Gov.Code § 12940(h).

[23] Civil Rights 78 1251

78 Civil Rights
78II Employment Practices
78k1241 Retaliation for Exercise of Rights
78k1251 k. Motive or intent; pretext. Most Cited Cases

Retaliatory animus need not be the sole factor motivating an adverse employment decision to establish a claim of retaliation in violation of California's Fair Employment and Housing Act (FEHA), but need only be a substantial or motivating factor. West's Ann.Cal.Gov.Code § 12940(h).

[24] Civil Rights 78 1245

78 Civil Rights
78II Employment Practices
78k1241 Retaliation for Exercise of Rights
78k1245 k. Adverse actions in general. Most Cited Cases

In determining whether an action or conduct rises to the level of retaliation in violation of California's Fair Employment and Housing Act (FEHA), a court must take into account the unique circumstances of the affected employee as well as the workplace context of the claim. West's Ann.Cal.Gov.Code § 12940(h).

[25] Civil Rights 78 1744

78 Civil Rights
78V State and Local Remedies
78k1742 Evidence
78k1744 k. Employment practices. Most Cited Cases

For a retaliation claim under California's Fair Employment and Housing Act (FEHA), intent to retaliate may be shown by either direct or circumstantial evidence. West's Ann.Cal.Gov.Code § 12940(h).

[26] Civil Rights 78 1244

78 Civil Rights
78II Employment Practices
78k1241 Retaliation for Exercise of Rights
78k1244 k. Activities protected. Most Cited Cases

Under California's Fair Employment and Housing Act (FEHA), an employer may not retaliate against an employee who opposed discrimination against a fellow employee, even if that employee was mistaken and there was no discrimination, so long as the mistake was sincere and reasonable. West's Ann.Cal.Gov.Code § 12940(h).

835 F.Supp.2d 762, 33 IER Cases 442
(Cite as: 835 F.Supp.2d 762)

[27] Federal Civil Procedure 170A 2497.1

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2497 Employees and Employment Discrimination, Actions Involving
170Ak2497.1 k. In general. Most Cited Cases

Genuine issue of material fact existed as to whether employees were subject to bullying and abuse after threatening to expose policy violations and practices of supervisors, precluding summary judgment in their claim alleging retaliation in violation of California's Fair Employment and Housing Act (FEHA). West's Ann.Cal.Gov.Code § 12940(h).

[28] Damages 115 57.21

115 Damages
115III Grounds and Subjects of Compensatory Damages
115III(A) Direct or Remote, Contingent, or Prospective Consequences or Losses
115III(A)2 Mental Suffering and Emotional Distress
115k57.19 Intentional or Reckless Infliction of Emotional Distress; Outrage
115k57.21 k. Elements in general. Most Cited Cases

The elements of a claim for intentional infliction of emotional distress (IIED) under California law are outrageous conduct by defendant, with the intention of causing, or reckless disregard of the probability of causing emotional distress, the plaintiff's suffering severe emotional distress and the actual and proximate causation of the emotional distress by the defendant's outrageous conduct.

[29] Damages 115 57.22

115 Damages
115III Grounds and Subjects of Compensatory Damages
115III(A) Direct or Remote, Contingent, or Prospective Consequences or Losses
115III(A)2 Mental Suffering and Emotional Distress
115k57.19 Intentional or Reckless Infliction of Emotional Distress; Outrage
115k57.22 k. Nature of conduct. Most Cited Cases

Damages 115 57.24

115 Damages
115III Grounds and Subjects of Compensatory Damages
115III(A) Direct or Remote, Contingent, or Prospective Consequences or Losses
115III(A)2 Mental Suffering and Emotional Distress
115k57.19 Intentional or Reckless Infliction of Emotional Distress; Outrage
115k57.24 k. Humiliation, insults, and indignities. Most Cited Cases

Conduct sufficient to sustain a claim of intentional infliction of emotional distress (IIED) under California law must be outrageous beyond the bounds of human decency; liability does not extend to mere insults, indignities, threats, annoyances, petty oppressions, or other trivialities.

[30] Federal Civil Procedure 170A 2515

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2515 k. Tort cases in general.

835 F.Supp.2d 762, 33 IER Cases 442
(Cite as: 835 F.Supp.2d 762)

Most Cited Cases

Genuine issue of material fact existed as to whether employees were subject to extreme and outrageous conduct, precluding summary judgment in their claims of intentional infliction of emotional distress (IIED)under California law.

***766** Mary Shea Hagebols, Shea Law Offices, Minal Jagdish Belani, Law Offices of Minal Belani, San Francisco, CA, for Plaintiffs.

Lawrence Hecimovich, City Attorney's Office, San Francisco, CA, for Defendants.

ORDER GRANTING IN PART AND DENYING IN PART MOTION FOR SUMMARY JUDGMENT

THELTON E. HENDERSON, District Judge.

This matter came before the Court on November 28, 2011, on a motion for summary judgment filed by Defendants City and County of San Francisco ("CCSF"). For the reasons set forth below, the motion is GRANTED as to Plaintiffs' second cause of action, and DENIED with regards to the remaining claims.

BACKGROUND

Plaintiffs Jane Doe and Anne Raskin, ("Doe" and "Raskin" or "Plaintiffs"), employees of Defendant City and County of San Francisco Department of Emergency Communications ("DEC"), contend that there has been a longstanding culture of bullying, hazing, and female-on-female gender-based harassment on the midnight shift of the DEC 911 dispatch. Following a long and intricate history of conflict between Plaintiff Doe and her supervisors, named as Defendants in this case, an incident involving Doe's personal email account brought the discord to a head in the fall and winter of 2009.

DEC provides a bank of computers for use by employees on their breaks, on which employees may check personal email and use the internet for non-work-related reasons, so long as they do not use the computers for any improper purpose. In October of 2009, 28 emails from Jane Doe's personal Yahoo! email account were printed by Defendants and submitted to the DEC's human resources department for review, based on (according to Defendants) the concern that the emails may contain confidential DEC personnel information, improperly disclosed by Doe to outside parties. According to Defendants, these emails were found by one of the Defendants when Doe left them open in multiple minimized windows on the shared workplace computer. According to Doe, the emails printed by Defendants were not open in minimized windows, but found by Defendant Madsen, who Doe claims searched through her inbox, sent mail, and folders to find emails containing potentially incendiary communications.

In December of 2009, Doe was informed of the emails received by human resources, during the course of their investigation (which ultimately did not find the emails violative of DEC policy). On October 14, ***767** 2010, Doe and Raskin (whose writings were also contained in the emails, as she had corresponded with Doe) filed suit, alleging violations of the Federal Stored Communications Act, California's whistleblower statutes, invasion of privacy, intentional infliction of emotional distress, as well as several California Fair Employment and Housing Act violations relating to gender-based discrimination, sexual harassment, and retaliatory conduct. On October 17, Defendants filed this motion for summary judgment, which we now consider.

LEGAL STANDARD

Summary judgment is appropriate when there is no genuine dispute as to material facts and the moving party is entitled to judgment as a matter of law. Fed.R.Civ.P. 56(c). Material facts are those that may affect the outcome of the case. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986). A dispute as to a material fact is "genuine" if there is sufficient evidence for a rea-

sonable jury to return a verdict for the nonmoving party. *Id.* The Court may not weigh the evidence and must view the evidence in the light most favorable to the nonmoving party. *Id.* at 255, 106 S.Ct. 2505. The Court's inquiry is "whether the evidence presents a sufficient disagreement to require submission to a jury or whether it is so one-sided that one party must prevail as a matter of law." *Id.* at 251–52, 106 S.Ct. 2505.

A party seeking summary judgment bears the initial burden of informing the Court of the basis for its motion, and of identifying those portions of the pleadings and discovery responses that "demonstrate the absence of a genuine issue of material fact." *Celotex Corp. v. Catrett*, 477 U.S. 317, 323, 106 S.Ct. 2548, 91 L.Ed.2d 265 (1986). Where the moving party will have the burden of proof at trial, it must "affirmatively demonstrate that no reasonable trier of fact could find other than for the moving party." *Soremekun v. Thrifty Payless, Inc.*, 509 F.3d 978, 984 (9th Cir.2007). However, on an issue for which its opponents will have the burden of proof at trial, the moving party can prevail merely by "pointing out ... that there is an absence of evidence to support the nonmoving party's case." *Celotex*, 477 U.S. at 325, 106 S.Ct. 2548. If the moving party meets its initial burden, the opposing party must "set out specific facts showing a genuine issue for trial" to defeat the motion. Fed.R.Civ.P. 56(e)(2); *Anderson*, 477 U.S. at 256, 106 S.Ct. 2505.

DISCUSSION

1. Federal Stored Communications Act

The Federal Stored Communications Act ("FSCA") provides a cause of action against any person or entity which "intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C. 2701. In order for a claim to be sustained, it must be shown that the individual made such access "with a knowing or intentional state of mind." 18 U.S.C. 2707(a).

In the Ninth Circuit, the act is akin to the tort of trespass, in that it "protects individuals' privacy and proprietary interests. The Act reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility." *Theofel v. Farey–Jones*, 359 F.3d 1066, 1072–1073 (9th Cir.2004).

Violations of the act have been found where individuals used electronic means to acquire the passwords of others and use those passwords to access their email accounts. *See* ***768***Miller v. Meyers*, 766 F.Supp.2d 919, 923 (W.D.Ark.2011) and *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp*, 759 F.Supp.2d 417, 423 (S.D.N.Y.2010).

[1] Here, the disagreement between the Defendants and Plaintiffs is twofold. The first disagreement pertains to the facts underlying this claim—while the Plaintiff contends that she did not leave her email open on the screen, the Defendants contend that Plaintiff did, in fact, leave open not just her inbox, but each individual email which was ultimately printed by Defendants. They contend that the individual emails were open and minimized at the bottom of the screen, and that the contents was only discovered in passing, as the emails were de-minimized by a Defendant co-worker who was simply closing the open windows. Plaintiff responds that this version of the facts is not true, and, in support of her contention, points out that the emails were pulled from various times over an 18–month period, and that it does not make sense that an individual checking their email would leave all these emails open-she contends that the emails must have been searched for in order to be discovered. Furthermore, she contends, the nature of the Windows XP program that was used on the shared computer on

which these emails were found makes it unlikely that these emails were all individual visible when minimized, as the program tends to "group" minimized windows.

The second point of disagreement is as to what would constitute violation of the act. Plaintiffs claim that searching through an already-open inbox is the kind of "access" that would violate the act, while Defendants contend that there can be no violation, as the individual who went through the email was simply doing so in the process of closing open windows, and lacked the mens rea to be in violation of the act.

The second point is heavily reliant on the first, as Defendants do not contend that, if the Plaintiffs' version of the facts is indeed correct, and there was a full search of Jane Doe's inbox, there would nevertheless be no violation of this statute. The position of the Defendants is that there was no search of this kind, and Plaintiffs refute this contention. Both sides have presented evidence in support of their version of events, and, therefore, there exists a genuine issue of material fact for the jury.

2. Privacy Claims

[2] "All people are by nature free and independent and have inalienable rights including the right of privacy." Cal. Const., art. I section 1. Article I, section 1 of the California Constitution creates a right of action against private parties and governmental entities. *Hill v. National Collegiate Athletic Ass'n.*, 7 Cal.4th 1, 20, 26 Cal.Rptr.2d 834, 865 P.2d 633 (1994). To establish a claim of violation of privacy under Article I, section 1 of the California Constitution, a plaintiff must show that defendants engaged in conduct which invaded plaintiff's privacy interest, that plaintiff had a reasonable expectation of privacy as to the interests invaded, that the invasion was serious and that the invasion caused plaintiff to suffer injury, damage, loss or harm. *Hill*, 7 Cal.4th at 32–37, 26 Cal.Rptr.2d 834, 865 P.2d 633.

[3][4] There are two recognized types of privacy interests: "informational privacy," which is the interest in precluding dissemination or misuse of sensitive or confidential information, and "autonomy privacy," which is the interest in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference. *Id.* at 35, 26 Cal.Rptr.2d 834, 865 P.2d 633. A public employee does not have a diminished expectation***769** of privacy in his or her personal information. *Long Beach City Employees Assn. v. City of Long Beach*,41 Cal.3d 937, 950–951, 227 Cal.Rptr. 90, 719 P.2d 660 (1986)

[5][6] A reasonable expectation of privacy is "an objective entitlement founded on broadly based and widely accepted community norms." *Sheehan v. San Francisco 49ers, Ltd.*, 45 Cal.4th 992, 1000, 89 Cal.Rptr.3d 594, 201 P.3d 472 (2009). Employees possess some reasonable expectation of privacy in data stored on work computers (*see U.S. v. Ziegler*, 474 F.3d 1184, 1190 (9th Cir.2007)) but "the use of computers in the employment context carries with it social norms that effectively diminish the employee's reasonable expectation of privacy with regard to the use of his employer's computers." *TBG Ins. Services Corp. v. Sup. Ct.*, 96 Cal.App.4th 443, 452, 117 Cal.Rptr.2d 155 (2002). In that case, an employee used his employer's computers to access sexually explicit material, and was fired. The Court held that since employers often monitor employees' computer use and the plaintiff knew his use could be monitored, he lacked any reasonable expectation of privacy. *Id.* at 452–45, 117 Cal.Rptr.2d 155.

[7] However, "Whether a legally recognized privacy interest exists is a question of law, and whether the circumstances give rise to a reasonable expectation of privacy and a serious invasion thereof are mixed questions of law and fact. If the undisputed material facts show no reasonable expectation of privacy or an insubstantial impact on privacy interests, the question of invasion may be adjudicated as a

matter of law." *Pioneer Electronics (USA), Inc. v. Superior Court*, 40 Cal.4th 360, 371–372, 53 Cal.Rptr.3d 513, 150 P.3d 198 (2007). The plaintiff contends that the emails are covered by the Meyers–Milias–Brown Act, Gov.Code section 3500 et seq., which ensures public employees' right to engage in a wide range of union-related activities without fear of sanction (gov. Code section 3506). Additionally, the circumstances at DEM are somewhat different than in the *TBG* case above, as the union rules, as contained in the Collective Bargaining Agreement between the City/County of SF and the Local 1021 contain a provision protecting the privacy interests of union members: "Employees subject to this Agreement shall have a reasonable expectation of privacy and to be secure from unreasonable searches and seizures on his/her person and his/her work area to the extent provided by law". In *TBG*, the plaintiff had signed a statement from his employer which disclosed the employer's policy of monitoring his email. In this case, no such policy existed.

[8] The Defendants argue that there was no reasonable expectation of privacy in this case, and, furthermore, that the emails were in plain view. They also contend that any invasion of Plaintiffs' privacy was not serious, citing *Hill*, 7 Cal.4th at 36–37, 26 Cal.Rptr.2d 834, 865 P.2d 633 for the proposition that in order to be considered serious, a violation must "constitute an egregious breach of the social norms underlying the privacy right." Plaintiffs respond that there was a reasonable expectation of privacy, citing the union rules listed above, and further argue that the invasion was clear and serious, as it involved an unauthorized access of Plaintiffs' email and resulted in "interference with and surveillance of Union activities." Plaintiffs further contend that they suffered emotional injury and harm because of the invasion, including humiliation, mental anguish and extreme distress.

Once again, as there is no agreement as to the facts underlying the "email incident," and that question is determinative in considering whether there was a reasonable expectation of privacy and whether it ***770** was invaded. The facts surrounding the role of the computer terminals at DEM, their use and their understood purpose, and the events surrounding the alleged invasion of Jane Doe's email account are clearly in dispute, and therefore summary judgment is not appropriate as to these claims.

3. California Labor Code Claims

The Defendants contend that these claims fail because Plaintiffs' failed to exhaust their administrative remedies. The Plaintiffs concede this point, and therefore summary judgment is GRANTED as to the Plaintiffs' second claim for relief, violations of California Labor Code sections 98.6, 1102.5, and 6310.

4. Gender Discrimination Claims

[9][10] In order to prevail on a claim of gender discrimination under California's Fair Employment and Housing Act, Cal. Government Code section 12900, ("FEHA") a plaintiff must prove that their managers acted with an intent to unlawfully discriminate against or harass them on the basis of their gender and that they suffered adverse employment action or, otherwise, that the alleged conduct was sufficiently severe and pervasive to alter the terms and conditions of their employment and create an abusive environment. *Oncale v. Sundowner Offshore Services, Inc.* 523 U.S. 75, 81, 118 S.Ct. 998, 140 L.Ed.2d 201 (1998); *Aguilar v. Avis Rent A Car System, Inc.*, 21 Cal.4th 121, 87 Cal.Rptr.2d 132, 980 P.2d 846 (1999) "The critical issue ... is whether members of one sex are exposed to disadvantageous terms or conditions of employment to which members of the other sex are not exposed." *Oncale*, 523 U.S. at 80–81, 118 S.Ct. 998.

[11][12][13][14] There is a three-stage burden-shifting test for discrimination claims in California. First, the Plaintiffs must show a *prima facie* case of discrimination. The plaintiff's burden is "not onerous" but "must at least show actions taken by the

employer from which one can infer, if such actions remained unexplained, that it is more likely than not that such actions were 'based on a [prohibited] discriminatory criterion.' Once the plaintiff establishes a prima facie case, a presumption of discrimination arises. This presumption, though "rebuttable," is 'legally mandatory.'... The ultimate burden of persuasion on the issue of actual discrimination remains with the plaintiff." *Guz v. Bechtel National, Inc.*, 24 Cal.4th 317, 354–356, 100 Cal.Rptr.2d 352, 8 P.3d 1089 (2000) (citations omitted). These facts may be proved circumstantially, from facts that create a reasonable likelihood of bias and are not satisfactorily explained. *Sandell v. Taylor–Listug, Inc.*, 188 Cal.App.4th 297, 307, 115 Cal.Rptr.3d 453 (2010). Furthermore, discriminatory animus need not be the sole motivation behind a challenged action: the plaintiff need only prove a " 'causal connection' between the employees protected status and adverse employment decision." *Mixon v. Fair Employment and Housing Com.*, 192 Cal.App.3d 1306, 1319, 237 Cal.Rptr. 884 (1987).

[15] Defendants argue that the Plaintiffs have not presented evidence that the alleged misconduct has to do with gender. They rely heavily on the fact that what is alleged here is woman-on-woman discrimination, which they seem to find improbable. They do not adequately address the fact that the Plaintiffs have discussed the difference between how men and women were treated in the workplace. The Plaintiffs contend that their deposition testimony is sufficient to meet the required showing that, had Plaintiffs been men, they would not have been treated in the same manner (referencing nearly verbatim the standard articulated in ***771***Accardi v. Superior Court*, 17 Cal.App.4th 341, 348, 21 Cal.Rptr.2d 292 (1993) on which Defendants rely). Again, if one believes Plaintiffs' contention that men were not expected to behave in a "subservient" manner, and not subjected to similar abusive conduct by their superiors, then it is reasonable to determine Plaintiffs' burden has been met. As the facts underlying this claim are in dispute, this is an issue proper for a jury determination, and not appropriate for determination on summary judgment.

5. Sexual Harassment Claim

[16][17] The laws prohibiting gender harassment are not intended as a "general civility code." *Oncale*, 523 U.S. at 81, 118 S.Ct. 998. Sporadic use of abusive language, gender-related jokes, occasional teasing, or isolated or trivial comments are not enough. *See Faragher v. City of Boca Raton*, 524 U.S. 775, 788, 118 S.Ct. 2275, 141 L.Ed.2d 662 (1998); *Etter v. Veriflo Corp.*, 67 Cal.App.4th 457, 465, 79 Cal.Rptr.2d 33 (1998). Rather, an employee must show "a concerted pattern of harassment of a repeated, routine or a generalized nature." *Lyle v. Warner Bros. TV. Prod.*, 38 Cal.4th 264, 283, 42 Cal.Rptr.3d 2, 132 P.3d 211 (2006).

[18] Furthermore, the harassment must create a hostile environment, which requires a showing of harassment sufficient that a reasonable person would consider it severe enough to alter the conditions of her employment or create an abusive working environment. *Fisher v. San Pedro*, 214 Cal.App.3d 590, 609, 262 Cal.Rptr. 842 (1989). Whether or not such a hostile work environment exists is to be determined only by considering all the circumstances involved. *Harris v. Forklift Systems, Inc.*, 510 U.S. 17, 23, 114 S.Ct. 367, 126 L.Ed.2d 295 (1993).

> Careful consideration [must be given] to the social context in which particular behavior occurs and how it is experienced by its target. The real social impact of workplace behavior depends on a constellation of surrounding circumstances, expectations, and relationships which are not fully captured by a simple recitation of the words used or the physical acts performed. Common sense, and appropriate sensitivity to social context will enable courts and juries to distinguish ... conduct which a reasonable person in the plaintiffs' position would find severely hostile and abusive.

Oncale, 523 U.S. at 81–82, 118 S.Ct. 998.

[19] Sexual harassment need not be sexual in nature. *Miller v. Department of Corrections*, 36 Cal.4th 446, 469, 30 Cal.Rptr.3d 797, 115 P.3d 77 (2005). Sexual favoritism may also constitute sexual harassment. *Id.* at 450–451, 30 Cal.Rptr.3d 797, 115 P.3d 77.

[20] Here, Defendants contend that the conduct described by Plaintiffs as sexual harassment is, in fact, nothing more than reprimands regarding their work, which, be they fair or unfair, are not sexual harassment. They argue that none of the conduct alleged by Plaintiffs, including disciplinary investigations which were never followed through, or other work-related hostility alleged by the Plaintiffs, is provably based on gender. Plaintiffs point to the case law allowing circumstantial proof of gender-based abuse and contend that the conduct they have alleged, taken in context, is sufficient.

The crux of the issue is a determination as to, first, whether the conduct alleged by Plaintiffs did, in fact, occur as they claim, and, second, whether or not the motive for the conduct was gender-related. Neither of these determinations is a question of law-both are actual disputes as to the material facts in the case, and therefore summary judgment is inappropriate as to this issue.

***772** *6. Failure to Prevent Claims*

[21] The entirety of Defendants' argument as to these claims is that there is no triable issue as to the discrimination, harassment or retaliation claims, and therefore there was no misconduct to be prevented. Therefore, if the Court finds that there is a triable issue as to these claims, the Defendants have made no other argument as to why this claim should be decided on summary judgment. Plaintiffs have addressed the issue in their briefing, pointing out that it is unlawful for an employer to "fail to take all reasonable steps necessary to prevent discrimination and harassment from occurring" (Cal. Gov.Code section 12940(k)) and that, despite Plaintiffs' numerous reports of discrimination, retaliation and harassment, the City and County of San Francisco did nothing to step in, and failed to investigate the complaints. The facts underlying this claim being disputed, summary judgment is inappropriate as to this issue.

7. Retaliation Claims

Defendants largely lump their retaliation argument in with their argument about Plaintiffs' whistleblower claims, which the Plaintiffs have conceded are barred by their failure to exhaust administrative remedies.

[22][23] Government Code section 12940(h) makes it an unlawful employment practice to "discriminate against any person because the person has opposed any practices forbidden under this part or because the person has filed a complaint, testified, or assisted in any proceeding under this part." A *prima facie* case of unlawful retaliation may be made by showing that (1) Plaintiff engaged in activities protected by the Fair Employment and Housing Act, (2) their employers subsequently took adverse employment action against them and (3) there was a causal connection between the protected activity and the adverse employment action. *Miller*, 36 Cal.4th at 472, 30 Cal.Rptr.3d 797, 115 P.3d 77 (2005). Retaliatory animus need not be the sole factor motivating the adverse employment decision, but need only be a substantial or motivating factor. *George v. California Unemployment Ins. Appeals Bd.*, 179 Cal.App.4th 1475, 1492, 102 Cal.Rptr.3d 431 (2009).

[24][25][26] In determining whether an action or conduct rises to this level, the Court must take into account the unique circumstances of the affected employee as well as the workplace context of the claim. *Yanowitz v. L'Oreal USA, Inc.*, 36 Cal.4th 1028, 1052, 32 Cal.Rptr.3d 436, 116 P.3d 1123 (2005). Negative references, performance reviews, and refusal to con-

sider for promotion have all been considered adverse employment actions. *Brooks v. City of San Mateo*, 229 F.3d 917, 928–929 (9th Cir.2000). Intent to retaliate may be shown by either direct or circumstantial evidence. *Colarossi v. Coty U.S. Inc.*, 97 Cal.App.4th 1142, 1153, 119 Cal.Rptr.2d 131 (2002). An employer may not retaliate against an employee who opposed discrimination against a fellow employee, even if that employee was mistaken and there was no discrimination, so long as the mistake was sincere and reasonable. *Flait v. North American Watch Corp.*, 3 Cal.App.4th 467, 477, 4 Cal.Rptr.2d 522 (Cal.App.2d Dist. 1992).

[27] Again, the disagreement between the parties is factual-the Plaintiff alleges that her threat to expose the policy violations and bad practices of her superiors resulted in bullying, abuse, and negative workplace treatment, while, though the Defendants presumably disagree with this contention, they devote their argument to Plaintiffs' failure to exhaust remedies. The argument brought by Defendants on this issue is undermined by the determination in ***773***Schifando v. City of Los Angeles*, 31 Cal.4th 1074, 6 Cal.Rptr.3d 457, 79 P.3d 569 (2003), in which the court held that an employee who has suffered employment-related discrimination is not required to exhaust the city's internal administrative remedy and the administrative remedy provided by FEHA before filing a FEHA discrimination claim.

8. Intentional Infliction of Emotional Distress

[28] The elements of a claim for intentional infliction of emotional distress ("IIED") are outrageous conduct by defendant, with the intention of causing, or reckless disregard of the probability of causing emotional distress; the plaintiff's suffering severe emotional distress and the actual and proximate causation of the emotional distress by the defendant's outrageous conduct. *Davidson v. City of Westminster*, 32 Cal.3d 197, 209–210, 185 Cal.Rptr. 252, 649 P.2d 894 (1982). Though Defendants assert that this claim duplicates the FEHA claims, it is established that a plaintiff may allege both employment discrimination and the additional injury of intentional infliction of emotional distress. *See Rojo v. Kliger*, 52 Cal.3d 65, 82, 276 Cal.Rptr. 130, 801 P.2d 373 (1990).

[29] Conduct sufficient to sustain a claim of IIED must be "outrageous beyond the bounds of human decency." *Janken v. GM Hughes Electronics*, 46 Cal.App.4th 55, 80, 53 Cal.Rptr.2d 741 (1996). "Liability does not extend to mere insults, indignities, threats, annoyances, petty oppressions, or other trivialities." *Fisher v. San Pedro Peninsula Hospital*, 214 Cal.App.3d 590, 617, 262 Cal.Rptr. 842 (1989).

[30] Here, Defendants contend that the conduct in question does not rise to the IIED standard, and was merely the rigorous, difficult training a dispatcher must go through, which sometimes involves abusive language. Plaintiffs respond that the "panoply of extreme and outrageous conduct that terrorized and tormented Plaintiff ... with the goal of causing her to suffer extreme duress, emotional distress, fright and intimidation" does, in fact, meet the IIED bar. Again, this is properly construed as a question of fact, entirely dependent on factual issues presently in dispute. It is not the Court's role to determine credibility, and therefore these factual disputes must be presented to a jury, and not determined on summary judgment.

CONCLUSION

For the reasons set forth above, the motion for summary judgment is GRANTED as to the second claim for relief, and DENIED as to the remaining claims.

IT IS SO ORDERED.

N.D.Cal.,2011.
Doe v. City and County of San Francisco
835 F.Supp.2d 762, 33 IER Cases 442

END OF DOCUMENT

906 F.Supp.2d 1017
(Cite as: 906 F.Supp.2d 1017)

United States District Court,
C.D. California.
Aaron MINTZ
v.
MARK BARTELSTEIN AND ASSOCIATES INC. et al.

Case Nos. 2:12–cv–02554–SVW–SS,
2:12–cv–03055–SVW–SS.
Nov. 1, 2012.

Background: Sports agent brought action against his former employer, seeking declaration that two provision of his employment contract were unenforceable. Agent filed separate complaint against employer and its principal, alleging violation of Computer Fraud and Abuse Act (CFAA) and California Data Access and Fraud Act (CDAFA), and various state law claims. Employer brought counterclaims against agent and his new employer, alleging various state claims, including breach of contract, breach of covenant of good faith and fair dealing, breach of duty of loyalty, and misappropriation of trade secrets. Agent and new employer moved for summary judgment.

Holdings: The District Court, Stephen V. Wilson, J., held that:
(1) agent lacked standing to seek declaratory relief;
(2) agent's email was not intercepted by former employer;
(3) former employer knowingly and without permission obtained data from agent's private email account;
(4) agent had legally protected privacy interest in terms of his employment with new employer;
(5) agent had reasonable expectation of privacy in his personal emails;
(6) former employer's hacking of agent's personal email account was serious invasion of privacy interest;
(7) agent lacked standing to sue former employer under California Unfair Business Practices Act; and
(8) there was no evidence that former employer owned mobile phone in agent's possession.

Motion granted in part and denied in part.

West Headnotes

[1] Declaratory Judgment 118A 61

118A Declaratory Judgment
118AI Nature and Grounds in General
118AI(D) Actual or Justiciable Controversy
118Ak61 k. Necessity. Most Cited Cases

Where a plaintiff seeks a declaration pursuant to the Declaratory Judgment Act, a district court must first inquire whether there is an actual case or controversy within its jurisdiction. 28 U.S.C.A. § 2201.

[2] Declaratory Judgment 118A 62

118A Declaratory Judgment
118AI Nature and Grounds in General
118AI(D) Actual or Justiciable Controversy
118Ak62 k. Nature and elements in general. Most Cited Cases

Declaratory Judgment 118A 64

118A Declaratory Judgment
118AI Nature and Grounds in General
118AI(D) Actual or Justiciable Controversy
118Ak64 k. Adverse interests or contentions. Most Cited Cases

In an action by a plaintiff seeking a declaration pursuant to the Declaratory Judgment Act, the question in each case is whether the facts alleged, under all the circumstances, show that there is a substantial controversy, between parties having adverse legal interests, of sufficient immediacy and reality to warrant the issuance of a declaratory judgment. 28 U.S.C.A. § 2201.

[3] Declaratory Judgment 118A 341.1

118A Declaratory Judgment
118AIII Proceedings
118AIII(E) Evidence
118Ak341 Presumptions and Burden of Proof
118Ak341.1 k. In general. Most Cited Cases

The burden is on the party seeking declaratory relief pursuant to the Declaratory Judgment Act to establish the existence of an actual controversy. 28 U.S.C.A. § 2201.

[4] Declaratory Judgment 118A 145

118A Declaratory Judgment
118AII Subjects of Declaratory Relief
118AII(G) Written Instruments and Contracts
118AII(G)1 In General
118Ak143 Particular Contracts
118Ak145 k. Employment and personal service contracts. Most Cited Cases

Declaratory Judgment 118A 301

118A Declaratory Judgment
118AIII Proceedings
118AIII(C) Parties
118Ak299 Proper Parties
118Ak301 k. Contracts. Most Cited Cases

There was no extant controversy with respect to noncompete clause in sports agent's employment contract with former employer, and thus, agent lacked standing to seek declaratory relief regarding clause pursuant to Declaratory Judgment Act, where there was no evidence that former employer had attempted to enforce clause. 28 U.S.C.A. § 2201.

[5] Declaratory Judgment 118A 145

118A Declaratory Judgment
118AII Subjects of Declaratory Relief
118AII(G) Written Instruments and Contracts
118AII(G)1 In General
118Ak143 Particular Contracts
118Ak145 k. Employment and personal service contracts. Most Cited Cases

Declaratory Judgment 118A 301

118A Declaratory Judgment
118AIII Proceedings
118AIII(C) Parties
118Ak299 Proper Parties
118Ak301 k. Contracts. Most Cited Cases

There was no extant controversy with respect to notice of termination provision in sports agent's employment contract with former employer, and thus, agent lacked standing to seek declaratory relief regarding provision pursuant to Declaratory Judgment Act. 28 U.S.C.A. § 2201.

[6] Telecommunications 372 1342

372 Telecommunications
372VIII Computer Communications
372k1339 Civil Liabilities; Illegal or Improper Purposes

372k1342 k. Fraud; unauthorized access or transmission. Most Cited Cases

There was no evidence that sports agent sustained a loss in excess of $5,000 as a result of his former employer hacking into his private email account, as required to support claim for violation of Computer Fraud and Abuse Act (CFAA) at summary judgment stage; although agent submitted evidence that he incurred over $25,000 in attorney fees and costs, such fees were paid not by agent, but his new employer, which was not victim of offense, there was no evidence that employee would be required to repay new employer, and litigation expenses did not qualify as a loss under the CFAA, as expenses incurred in discovering identity of the offender litigation costs in question were not essential to remedying harm of unauthorized access. 18 U.S.C.App.(2006 Ed.) § 1030(a).

[7] Telecommunications 372 1439

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General
372k1435 Acts Constituting Interception or Disclosure
372k1439 k. Computer communications. Most Cited Cases

Sports agent's email was not intercepted by former employer within meaning of Electronic Communications and Privacy Act (ECPA) provisions prohibiting intentional interception of electronic communication, intentional disclosure of electronic communication known to have been obtained through interception, and intentional use of contents of electronic communication known to have been obtained through interception; employer did not access, disclose, or use any emails that had been acquired during transmission, rather, emails employer viewed were stored on agent's private email account. 18 U.S.C.A. § 2511(1)(a, c, d).

[8] Telecommunications 372 1439

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General
372k1435 Acts Constituting Interception or Disclosure
372k1439 k. Computer communications. Most Cited Cases

For an email to be "intercepted" in violation of the Electronic Communications Privacy Act (ECPA), it must be acquired during transmission, not while it is in electronic storage. 18 U.S.C.A. § 2511(1)(a, c, d).

[9] Telecommunications 372 1342

372 Telecommunications
372VIII Computer Communications
372k1339 Civil Liabilities; Illegal or Improper Purposes
372k1342 k. Fraud; unauthorized access or transmission. Most Cited Cases

Sports agent's former employer knowingly and without permission used a computer to wrongfully obtain data from agent's private email account, in violation of California statute prohibiting such conduct, where, at the direction of employer's senior counsel, an employee accessed agent's account without permission, and viewed contents of several emails, including agent's employment agreement with new employer. West's Ann.Cal.Penal Code § 502(c)(1), (e)(1).

[10] Action 13 5

13 Action
13I Grounds and Conditions Precedent
13k5 k. Criminal acts. Most Cited Cases

Telecommunications 372 1346

372 Telecommunications
372VIII Computer Communications
372k1339 Civil Liabilities; Illegal or Improper Purposes
372k1346 k. Actions. Most Cited Cases

Sports agent experienced sufficient damage to support private right of action against former employer for violation of California statute prohibiting use of another's data or computer network without permission, where, after employer hacked into agent's private email account, agent spent some time restoring his email account password and investigating who had hacked the account. West's Ann.Cal.Penal Code § 502(c)(1), (e)(1).

[11] Constitutional Law 92 1210

92 Constitutional Law
92XI Right to Privacy
92XI(A) In General
92k1210 k. In general. Most Cited Cases

Constitutional Law 92 1215

92 Constitutional Law
92XI Right to Privacy
92XI(A) In General
92k1215 k. Reasonable, justifiable, or legitimate expectation. Most Cited Cases

To prevail on a claim for a violation of the right to privacy under the California Constitution, a plaintiff must establish (1) a legally protected privacy interest, (2) a reasonable expectation of privacy under the circumstances, and (3) a serious invasion of the privacy interest. West's Ann.Cal. Const. Art. 1, § 1.

[12] Constitutional Law 92 963

92 Constitutional Law
92VI Enforcement of Constitutional Provisions
92VI(C) Determination of Constitutional Questions
92VI(C)1 In General
92k963 k. Questions of law or fact. Most Cited Cases

Under California law, whether a legally recognized privacy interest is present in a given case is a question of law to be decided by the court. West's Ann.Cal. Const. Art. 1, § 1.

[13] Constitutional Law 92 963

92 Constitutional Law
92VI Enforcement of Constitutional Provisions
92VI(C) Determination of Constitutional Questions
92VI(C)1 In General
92k963 k. Questions of law or fact. Most Cited Cases

Under California law, whether a plaintiff has a reasonable expectation of privacy in the circumstances and whether defendant's conduct constitutes a serious invasion of privacy are mixed questions of law and fact; if the undisputed material facts show no reasonable expectation of privacy or an insubstantial impact on privacy interests, the question of invasion may be adjudicated as a matter of law. West's Ann.Cal. Const. Art. 1, § 1.

[14] Constitutional Law 92 1210

92 Constitutional Law

92XI Right to Privacy
92XI(A) In General
92k1210 k. In general. Most Cited Cases

Under California law, invasion of a privacy interest is not a violation of the state constitutional right to privacy if the invasion is justified by a competing interest. West's Ann.Cal. Const. Art. 1, § 1.

[15] Constitutional Law 92 1210

92 Constitutional Law
92XI Right to Privacy
92XI(A) In General
92k1210 k. In general. Most Cited Cases

Under California law, conduct alleged to be an invasion of privacy under the state constitution is to be evaluated based on the extent to which it furthers legitimate and important competing interests. West's Ann.Cal. Const. Art. 1, § 1.

[16] Constitutional Law 92 1228

92 Constitutional Law
92XI Right to Privacy
92XI(B) Particular Issues and Applications
92k1227 Records or Information
92k1228 k. In general. Most Cited Cases

The protection of one's personal financial affairs against compulsory public disclosure is an aspect of the zone of privacy which is protected by the Fourth Amendment and which also falls within that penumbra of constitutional rights into which the government may not intrude absent a showing of compelling need and that the intrusion is not overly broad. U.S.C.A. Const.Amend. 4.

[17] Constitutional Law 92 1228

92 Constitutional Law
92XI Right to Privacy
92XI(B) Particular Issues and Applications
92k1227 Records or Information
92k1228 k. In general. Most Cited Cases

Under California law, individuals have a legitimate privacy interest protected by the state constitution with respect to income earned in the private sector. West's Ann.Cal. Const. Art. 1, § 1.

[18] Constitutional Law 92 1228

92 Constitutional Law
92XI Right to Privacy
92XI(B) Particular Issues and Applications
92k1227 Records or Information
92k1228 k. In general. Most Cited Cases

Torts 379 332

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)1 Privacy in General
379k332 k. Particular cases in general. Most Cited Cases

Under California law, sports agent had legally protected privacy interest in terms of his employment with new employer, including his compensation, as required to support claim against former employer for violation of his right to privacy under California Constitution. West's Ann.Cal. Const. Art. 1, § 1.

[19] Constitutional Law 92 1228

92 Constitutional Law
92XI Right to Privacy
92XI(B) Particular Issues and Applications
92k1227 Records or Information

92k1228 k. In general. Most Cited Cases

Torts 379 341

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)2 Intrusion
379k341 k. Particular cases in general. Most Cited Cases

Sports agent had reasonable expectation of privacy in his personal emails, as required to support claim against former employer for violation of his right to privacy under California Constitution based on employer hacking into his personal email account; hacked email account was web-based personal email account, agent had been sole account holder since he opened account, agent only forwarded email from business account to personal account when it contained personal matters or if he needed to print document away from office, personal account was password protected at all times, and agent had never authorized any of employer's employees to authorize it. West's Ann.Cal. Const. Art. 1, § 1.

[20] Constitutional Law 92 1210

92 Constitutional Law
92XI Right to Privacy
92XI(A) In General
92k1210 k. In general. Most Cited Cases

Under California law, actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right. West's Ann.Cal. Const. Art. 1, § 1.

[21] Constitutional Law 92 1228

92 Constitutional Law
92XI Right to Privacy
92XI(B) Particular Issues and Applications
92k1227 Records or Information
92k1228 k. In general. Most Cited Cases

Torts 379 341

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)2 Intrusion
379k341 k. Particular cases in general. Most Cited Cases

Under California law, employer's hacking of former employee's personal email account was serious invasion of privacy interest, as required to support employee's claim against employer for violation of his right to privacy under California Constitution, where another employee accessed former employee's private email account without permission at the direction of employer's counsel, and other employee opened several personal emails before reading former employee's employment agreement with new employer. West's Ann.Cal. Const. Art. 1, § 1.

[22] Antitrust and Trade Regulation 29T 290

29T Antitrust and Trade Regulation
29TIII Statutory Unfair Trade Practices and Consumer Protection
29TIII(E) Enforcement and Remedies
29TIII(E)1 In General
29Tk287 Persons Entitled to Sue or Seek Remedy
29Tk290 k. Private entities or individuals. Most Cited Cases

A private plaintiff has standing to sue under California Unfair Business Practices Act only if he has suffered injury in fact and has lost money or property

as a result of such unfair competition.

[23] Antitrust and Trade Regulation 29T 290

29T Antitrust and Trade Regulation
29TIII Statutory Unfair Trade Practices and Consumer Protection
29TIII(E) Enforcement and Remedies
29TIII(E)1 In General
29Tk287 Persons Entitled to Sue or Seek Remedy
29Tk290 k. Private entities or individuals. Most Cited Cases

There was no evidence that sports agent lost any money or property as a result of his former employer's violations of other laws, and thus, agent lacked standing to sue former employer under California Unfair Business Practices Act. West's Ann.Cal.Bus. & Prof.Code § 17200.

[24] Contracts 95 326

95 Contracts
95VI Actions for Breach
95k326 k. Grounds of action. Most Cited Cases

Under California law, the elements of a cause of action for breach of contract are: (1) the existence of the contract, (2) plaintiff's performance or excuse for nonperformance, (3) defendant's breach, and (4) the resulting damages to the plaintiff.

[25] Federal Civil Procedure 170A 2497.1

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2497 Employees and Employment Discrimination, Actions Involving
170Ak2497.1 k. In general. Most Cited Cases

There was no evidence that sports agent's former employer suffered damages as a result of any breach of agent's employment contract, as required to support breach of contract claim under California law at summary judgment stage; although former employer alleged that agent communicated with at least two recruits while working for former employer, and instead signed their deals while working for new employer, such bare allegation neglected to cite relevant facts in record that supported assertion, and there was no evidence in record that two recruits were now clients with agent's new employer.

[26] Labor and Employment 231H 153(4)

231H Labor and Employment
231HIII Rights and Duties of Employers and Employees in General
231Hk143 Actions by Employer Against Employee
231Hk153 Evidence
231Hk153(4) k. Weight and sufficiency. Most Cited Cases

There was no evidence that sports agent's former employer suffered damages as a result of agent's failure to give 14 days' notice of his resignation pursuant to employment agreement, as required to support breach of contract claim under California law based on failure to give adequate notice; although former employer asserted that because of lack of notice, it was unable to contact a client until five days after agent's resignation, client remained with employer, and employer did not identify single client that it lost as result of agent's failure to give notice.

[27] Pleading 302 64(2)

302 Pleading
302II Declaration, Complaint, Petition, or Statement
302k64 Duplicity
302k64(2) k. Particular causes or grounds of action. Most Cited Cases

Under California law, where allegations of breach of the covenant of good faith do not go beyond the statement of a mere contract breach and, relying on the same alleged acts, simply seek the same damages or other relief already claimed in a companion contract cause of action, they may be disregarded as superfluous as no additional claim is actually stated.

[28] Fraud 184 7

184 Fraud
184I Deception Constituting Fraud, and Liability Therefor
184k5 Elements of Constructive Fraud
184k7 k. Fiduciary or confidential relations. Most Cited Cases

To establish a claim for breach of the duty of loyalty under California law, a plaintiff must demonstrate: (1) the existence of a relationship giving rise to a duty of loyalty; (2) one or more breaches of that duty; and (3) damage proximately caused by that breach.

[29] Labor and Employment 231H 114(1)

231H Labor and Employment
231HIII Rights and Duties of Employers and Employees in General
231Hk109 Employee's Duties
231Hk114 Conflict of Interest
231Hk114(1) k. In general. Most Cited Cases

Under California law, an employee does not breach his duty of loyalty merely by preparing to compete with his employer.

[30] Labor and Employment 231H 114(1)

231H Labor and Employment
231HIII Rights and Duties of Employers and Employees in General
231Hk109 Employee's Duties
231Hk114 Conflict of Interest
231Hk114(1) k. In general. Most Cited Cases

While some preparation is permitted, California law does not authorize an employee to transfer his loyalty to a competitor.

[31] Labor and Employment 231H 153(4)

231H Labor and Employment
231HIII Rights and Duties of Employers and Employees in General
231Hk143 Actions by Employer Against Employee
231Hk153 Evidence
231Hk153(4) k. Weight and sufficiency. Most Cited Cases

Under California law, there was no evidence that sports agent transferred his loyalty to new employer before his resignation with former employer, as required to support claim for breach of duty of loyalty.

[32] Labor and Employment 231H 153(4)

231H Labor and Employment
231HIII Rights and Duties of Employers and Employees in General
231Hk143 Actions by Employer Against Employee
231Hk153 Evidence

231Hk153(4) k. Weight and sufficiency. Most Cited Cases

Under California law, there was no evidence that sports agent's former employer suffered damages as result of agent preparing to compete with former employer by working for new employer, as required to support claim for breach of duty of loyalty.

[33] Antitrust and Trade Regulation 29T 414

29T Antitrust and Trade Regulation
29TIV Trade Secrets and Proprietary Information
29TIV(A) In General
29Tk414 k. Elements of misappropriation. Most Cited Cases

A claim for misappropriation of trade secrets in violation of California's Uniform Trade Secrets Act has three core elements: (1) the plaintiff owned a trade secret, (2) the defendant acquired, disclosed, or used the plaintiff's trade secret through improper means, and (3) the defendant's actions damaged the plaintiff. West's Ann.Cal.Civ.Code § 3426.1(b).

[34] Antitrust and Trade Regulation 29T 420

29T Antitrust and Trade Regulation
29TIV Trade Secrets and Proprietary Information
29TIV(A) In General
29Tk420 k. Particular cases, in general. Most Cited Cases

There was no evidence of any specific instance of misappropriation of trade secrets by sports agent, as required to support former employer's claim for misappropriation of trade secrets in violation of California's Uniform Trade Secrets Act. West's Ann.Cal.Civ.Code § 3426.1.

[35] Torts 379 212

379 Torts
379III Tortious Interference
379III(B) Business or Contractual Relations
379III(B)1 In General
379k212 k. Contracts. Most Cited Cases

In the usual case, to prove intentional interference with contractual relations under California law, a plaintiff must demonstrate: (1) a valid contract between plaintiff and a third party; (2) defendant's knowledge of this contract; (3) defendant's intentional acts designed to induce a breach or disruption of the contractual relationship; (4) actual breach or disruption of the contractual relationship; and (5) resulting damage.

[36] Labor and Employment 231H 904

231H Labor and Employment
231HIX Interference with the Employment Relationship
231Hk904 k. Elements. Most Cited Cases

Under California law, to recover for a defendant's interference with an at-will employment relation, a plaintiff must plead and prove that the defendant engaged in an independently wrongful act, i.e., an act proscribed by some constitutional, statutory, regulatory, common law, or other determinable legal standard, that induced an at-will employee to leave the plaintiff.

[37] Labor and Employment 231H 909

231H Labor and Employment
231HIX Interference with the Employment Relationship
231Hk907 Enticing Employee to Leave Employment
231Hk909 k. Competitors. Most Cited Cases

There was no evidence that sports agent's new employer committed any independently wrongful act to induce agent to breach or disrupt his at-will employment contract with former employer, as required to support claim for interference with contractual relations under California law.

[38] Torts 379 213

379 Torts
379III Tortious Interference
379III(B) Business or Contractual Relations
379III(B)1 In General
379k213 k. Prospective advantage, contract or relations; expectancy. Most Cited Cases

Under California law, the elements of a claim for intentional interference with prospective economic advantage mirror those for intentional interference with an at-will employment contract, including the requirement that the plaintiff establish that the defendant engaged in an independently wrongful act, that is, if it is proscribed by some constitutional, statutory, regulatory, common law, or other determinable legal standard.

[39] Conversion and Civil Theft 97C 100

97C Conversion and Civil Theft
97CI Acts Constituting and Liability Therefor
97Ck100 k. In general; nature and elements. Most Cited Cases

Conversion has three elements under California Law: (1) ownership or right to possession of property; (2) wrongful disposition of the property right; and (3) damages.

[40] Conversion and Civil Theft 97C 124

97C Conversion and Civil Theft
97CII Actions
97CII(A) Right of Action and Defenses
97Ck123 Title and Right to Possession of Plaintiff
97Ck124 k. In general. Most Cited Cases

There was no evidence that sports agent's former employer owned mobile phone in agent's possession, as required to support employer's conversion claim under California law.

[41] Telecommunications 372 1342

372 Telecommunications
372VIII Computer Communications
372k1339 Civil Liabilities; Illegal or Improper Purposes
372k1342 k. Fraud; unauthorized access or transmission. Most Cited Cases

There was no evidence that sports agent's former employer was damaged by agent forwarding employer data to his personal email account, as required to support employer's claim against agent for accessing its computers without permission and copying or deleting date in violation of California statute prohibiting such conduct. West's Ann.Cal.Penal Code § 502.

[42] Federal Civil Procedure 170A 2553

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)3 Proceedings
170Ak2547 Hearing and Determination
170Ak2553 k. Time for consideration of motion. Most Cited Cases

A party seeking further discovery at the summary

judgment stage must show that (1) it has set forth in affidavit form the specific facts it hopes to elicit from further discovery; (2) the facts sought exist; and (3) the sought-after facts are essential to oppose summary judgment. Fed.Rules Civ.Proc.Rule 56(d)(2), 28 U.S.C.A.

[43] Federal Civil Procedure 170A 2546

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)3 Proceedings
170Ak2542 Evidence
170Ak2546 k. Weight and sufficiency. Most Cited Cases

A nonmoving party cannot avoid summary judgment by relying solely on conclusory allegations that are unsupported by factual data.

[44] Federal Civil Procedure 170A 2553

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)3 Proceedings
170Ak2547 Hearing and Determination
170Ak2553 k. Time for consideration of motion. Most Cited Cases

Sports agent's former employer was not entitled to continuance for further discovery at summary judgment stage of defamation action against agent; employer's request for continuance did not identify specific facts that further discovery would have revealed or explain why those facts would have precluded summary judgment. Fed.Rules Civ.Proc.Rule 56(d)(2), 28 U.S.C.A.

[45] Conspiracy 91 1.1

91 Conspiracy
91I Civil Liability
91I(A) Acts Constituting Conspiracy and Liability Therefor
91k1 Nature and Elements in General
91k1.1 k. In general. Most Cited Cases

Standing alone, a conspiracy does no harm and engenders no tort liability under California law; it must be activated by the commission of an actual tort.

[46] Conspiracy 91 6

91 Conspiracy
91I Civil Liability
91I(A) Acts Constituting Conspiracy and Liability Therefor
91k1 Nature and Elements in General
91k6 k. Damage caused. Most Cited Cases

Under California law, a civil conspiracy, however atrocious, does not give rise to a cause of action unless a civil wrong has been committed resulting in damage.

[47] Antitrust and Trade Regulation 29T 135(1)

29T Antitrust and Trade Regulation
29TIII Statutory Unfair Trade Practices and Consumer Protection
29TIII(A) In General
29Tk133 Nature and Elements
29Tk135 Practices Prohibited or Required
29Tk135(1) k. In general; unfairness. Most Cited Cases

Antitrust and Trade Regulation 29T 135(2)

29T Antitrust and Trade Regulation

29TIII Statutory Unfair Trade Practices and Consumer Protection
29TIII(A) In General
29Tk133 Nature and Elements
29Tk135 Practices Prohibited or Required
29Tk135(2) k. Source of prohibition or obligation; lawfulness. Most Cited Cases

Antitrust and Trade Regulation 29T 136

29T Antitrust and Trade Regulation
29TIII Statutory Unfair Trade Practices and Consumer Protection
29TIII(A) In General
29Tk133 Nature and Elements
29Tk136 k. Fraud; deceit; knowledge and intent. Most Cited Cases

Because California's Unfair Competition Law is written in the disjunctive, it establishes three varieties of unfair competition: acts or practices which are unlawful, or unfair, or fraudulent; in other words, a practice is prohibited as unfair or deceptive even if not unlawful and vice versa. West's Ann.Cal.Bus. & Prof.Code § 17200.

***1023** Anthony J. Oncidi, Robert H. Horn, Susan L. Gutierrez, Proskauer Rose LLP, Daniel Stephen Miller, Louis R. Miller, Miller Barondess, Los Angeles, CA, Christopher L. Williams, Proskauer Rose LLP, New Orleans, LA, for Aaron Mintz.

Adrian M. Pruetz, Paul Benedict Salvaty, Christopher Dacus, G. Jill Basinger, Lauren M. Gibbs, Glaser Weil Fink Jacobs Howard Avchen and Shapiro LLP, Los Angeles, CA, for Mark Bartelstein and Associates Inc.

STEPHEN V. WILSON, District Judge.

Proceedings: IN CHAMBERS ORDER re:

[48] MOTION for Summary Judgment as to All Counterclaims or, alternatively, MOTION for Partial Summary Judgment as to declaratory relief; violation of the Computer Fraud and Abuse Act; violation of the Electronic Communications and Privacy Act; violation of California Penal Code § 502; invasion of privacy; unfair business practices under state law; and all counterclaims filed by Plaintiff and Counterdefendants Creative Artists Agency LLC, Aaron L Mintz;

[56] MOTION for Partial Summary Judgment filed by Defendants and Counterclaimants Mark Bartelstein and Associates Inc.

I. INTRODUCTION

This case arises from the departure of a basketball sports agent from his old agency, Mark Bartelstein & Associates, Inc. d/b/a Priority Sports & Entertainment ("Priority Sports"), to join the Creative Arts Agency ("CAA"). On March 23, 2012, Plaintiff Aaron Mintz ("Plaintiff") filed the instant action against his erstwhile employer, Priority Sports, seeking a declaration under the Declaratory Judgment Act, 28 U.S.C. § 2201, that two provisions of Plaintiff's employment contract with Priority Sports are unenforceable, namely a two-year non-compete clause and the requirement of fourteen days' written notice of termination. (Compl. I ¶¶ 15–16).

***1024** On April 6, 2012, Plaintiff filed a separate complaint against Priority Sports and its principal, Mark Bartelstein (collectively, "Defendants"), alleging that following Plaintiff's resignation, Defendants had engaged in a course of illegal retaliatory conduct, which included acquiring unauthorized access to Plaintiff's personal emails, obtaining confidential information about the terms of Plaintiff's employment with CAA, and disclosing this information to third parties. (Compl. II ¶ 1). Thus, the second complaint advances the following causes of action: (1) violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030; (2) violation of the Electronic Communications and Privacy Act ("EPCA"), 18 U.S.C. §§

2510 et seq.; (3) violation of the California Data Access and Fraud Act ("CDAFA"), Cal.Penal Code § 502; (4) defamation; (5) invasion of privacy; (6) interference with prospective economic relations; and (7) violation of the California Unfair Business Practices Act ("UCL"), Cal. Bus. & Prof.Code §§ 17200 et seq.[FN1]

FN1. This complaint initially was filed under a separate case number, 2:12–cv–03055–SVW–SS. On June 11, 2012, the Court consolidated Plaintiff's two complaints into a single case, with the first-filed action being the lead case. (Dkt. 19).

On April 17, 2012, Priority Sports counterclaimed alleging that before and after his resignation, Plaintiff conspired with CAA to misappropriate Priority Sports' confidential information, to convert Priority Sports' clientele to CAA, and to breach the terms of Plaintiff's employment contract with Priority Sports. (Counterclaim ¶¶ 3–4). Priority Sports accordingly asserts the following counterclaims: (1) breach of contract against Mintz; (2) breach of the covenant of good faith and fair dealing against Plaintiff; (3) breach of the duty of loyalty against Plaintiff; (4) misappropriation of trade secrets against Plaintiff and CAA (collectively, "Counterdefendants"); (5) intentional interference with contractual relations as to CAA; (6) intentional interference with present and prospective economic advantage and business relationships against Counterdefendants; (7) conversion against Plaintiff; (8) violation of California Penal Code § 502 against Plaintiff; (9) defamation against Plaintiff; (10) trade libel against Plaintiff; (11) conspiracy against Counterdefendants; and (12) violation of the UCL against Counterdefendants. (Dkt. 9).

On October 1, 2012, Plaintiff and CAA filed the instant Motion for Summary Judgment as to all Defendants' counterclaims, or in the alternative, Motion for Partial Summary Judgment on Plaintiff's claims with respect to the Declaratory Judgment Act, the CFAA, the ECPA, California Penal Code § 502, invasion of privacy, and unfair competition. (Dkt. 48).[FN2] Defendants simultaneously filed a Motion for Partial Summary Judgment as to their claims against Plaintiff for breach of contract and breach of the duty of loyalty. (Dkt. 56).

FN2. In other words, the Motion does not seek summary judgment on the claims for defamation and the interference with prospective economic advantage.

For the reasons below, Plaintiff's Motion for Summary Judgment on its own claims is GRANTED with respect to the claims for violation of California Penal Code § 502 and invasion of privacy, but DENIED with respect to the claim under the UCL. Further, the Court GRANTS summary judgment in favor of Defendants on Plaintiff's claims for declaratory relief, violation of the CFAA, and violation of the ECPA. Counterdefendants' Motion for Summary Judgment as to Defendants' counterclaims is GRANTED as to every claim. Accordingly, Defendants' Motion ***1025** for Partial Summary Judgment is DENIED as moot.

II. FACTS

A. Plaintiff's Employment Contract with Priority Sports

Priority Sports is a Chicago-based sports agency that represents professional athletes. Plaintiff worked in Priority Sports' Los Angeles office for eleven years, from September 25, 2001 until March 23, 2012. When he began working for Priority Sports, Plaintiff signed an employment contract. Pursuant to the employment agreement, Plaintiff agreed:

> (1) To devote all working time, knowledge, skill, attention, and energy, using his best efforts, to the

duties and responsibilities set forth herein;

(2) To serve and further the interest of the Company in every lawful way; and

(3) To follow the Company's policies and directives, and any modifications thereof.

(Compl. I, Ex. A ¶ II(A)). Plaintiff further agreed: that during the Employee's employment with the Company the Employee will not, directly or indirectly, on behalf of himself or others either as an employee, consultant, owner, independent contractor or in any other capacity whatsoever:

1. Solicit Company Clients or business on behalf of a Company Competitor;

2. Recruit Company employees on behalf of a Company Competitor;

3. Perform or engage in activities or in the provision of services, in any capacity, on behalf of or for a Company Competitor;

... or

5. Disclose Confidential Business Information to anyone, including, without limitation, Company Competitors not affiliated with the Company, without the Company's prior written consent.

(*Id.* ¶ II(B)).

The employment contract also set forth specific terms concerning termination and its aftermath. Section IV(D) states that Plaintiff "may terminate his employment with the Company for any reason or no reason upon fourteen (14) days' written notice to the Company." (*Id.* ¶ IV(D)). Further, Section V(A) sets forth what is referred to by the parties as the non-compete provision:

For two (2) years following the termination of the Employee's employment, regardless of the reason therefore, the Employee agrees that the Employee will not, directly or indirectly, on behalf of himself or others either as an employee, consultant, owner, independent contractor or in any other capacity whatsoever:

1. Solicit Company Clients;

2. Recruit Company employees for or on behalf of Company Competitors:

3. Disclose Confidential Business Information to persons not affiliated with the Company, including, without limitation, Company Competitors, without the Company's prior written consent; or

4. Provide, or assist in providing, either directly or through a Company Competitor, services that are, or are similar to the services, provided by the Company to a Company Client.

(*Id.* ¶ V(A)). Finally, the employment contract provides that:

Upon and after the termination of Employee's employment, regardless of the reason therefor, the Employee shall not copy, duplicate, and/or remove documents containing Confidential Business Information from Company offices, and the Employee will promptly return to ***1026** the Company any such documents the Employee possesses.

(*Id.* ¶ V(B)).

B. Plaintiff's Resignation from Priority Sports

In early March 2012, CAA offered Plaintiff a job. It is undisputed that on March 23, 2012, Plaintiff terminated his employment with Priority Sports without giving fourteen days' written notice. (Def.

Response to Pl. Uncontroverted Facts ("DUF") 6). That evening, Plaintiff spoke on the telephone with Bartelstein and informed him of his resignation. Bartelstein allegedly concluded the conversation by saying, "Wait until I tell the world about this. You made your bed, you better be ready to lie in it." (Mintz Decl. ¶ 15).

C. Defendants' Alleged Retaliation Against Plaintiff

On March 25, 2012, Priority Sports' General Counsel, Rick Smith, instructed another employee, Bradley Ames, to access Plaintiff's personal email account (a.k.a. the "Gmail account") without Plaintiff's permission. (DUF 7–10). Ames obtained a temporary password without Plaintiff's consent and accessed Plaintiff's Gmail account for at least twenty minutes. (DUF 11). It is undisputed that Ames viewed a copy of Plaintiff's employment agreement with CAA. (DUF 12). The next day, Plaintiff's colleague, Kevin Zuckerman, emailed Plaintiff the following message: "I'm in shock! Rumor on the street is that CAA is paying you less money over 4 years then [sic] you would have made here. I don't get it[.] You had a 50–year guaranteed deal here." (DUF 15). Plaintiff contends that Defendants leaked his employment terms with CAA to a third party named Josh Ketroser. (DUF 16). Plaintiff further alleges that Bartelstein subsequently defamed him in front of various NBA team executives and players to persuade them not to follow Plaintiff to CAA. (Mot. at 6).

D. Plaintiff and CAA's Alleged Misconduct

Defendants first claim that Plaintiff breached his employment by failing to give fourteen days' written notice of his resignation effective March 23, 2012. In addition, Defendants assert that during Plaintiff's negotiations with CAA, and while Plaintiff was still employed by Priority Sports, he provided CAA with a copy of his employment contract with Priority Sports. Bartelstein also attested in his declaration that prior to his resignation, Plaintiff failed to inform Priority Sports that a client's relative had complained about the company's marketing department. (Bartelstein Decl. ¶ 10). Bartelstein further claims that prior to his resignation, Plaintiff failed to advise Priority Sports about (1) his communications with a prospective client named Mike Scott, (2) his attempted communications with prospective client Terrence Ross and his family; and (3) his communications with another prospective client, Rob Sacre. (*Id.* ¶¶ 11–12).

III. LEGAL STANDARD

Rule 56(c) requires summary judgment for the moving party when the evidence, viewed in the light most favorable to the nonmoving party, shows that there is no genuine issue as to any material fact, and that the moving party is entitled to judgment as a matter of law. *See* Fed.R.Civ.P. 56(c); *Tarin v. County of Los Angeles*, 123 F.3d 1259, 1263 (9th Cir.1997).

The moving party bears the initial burden of establishing the absence of a genuine issue of material fact. *See Celotex Corp. v. Catrett*, 477 U.S. 317, 323–24, 106 S.Ct. 2548, 91 L.Ed.2d 265 (1986). "When the party moving for summary judgment ***1027** would bear the burden of proof at trial, it must come forward with evidence which would entitle it to a directed verdict if the evidence went uncontroverted at trial." *C.A.R. Transp. Brokerage Co., Inc. v. Darden Rests., Inc.*, 213 F.3d 474, 480 (9th Cir.2000) (internal quotations and citations omitted). However, if the moving party does not bear the burden of proof, it can satisfy its Rule 56(c) burden by " 'showing'—that is, pointing out to the district court—that there is an absence of evidence to support the nonmoving party's case." *Celotex*, 477 U.S. at 325, 106 S.Ct. 2548. Either way, if the moving party fails to meet its initial burden, summary judgment must be denied and the court need not consider the nonmoving party's evidence. *See Adickes v. S.H. Kress & Co.*, 398 U.S. 144, 159–60, 90 S.Ct. 1598, 26 L.Ed.2d 142 (1970).

If the moving party meets its initial burden, the nonmoving party must identify specific facts, drawn from the materials on file, that show that an issue is

genuinely disputed. *See Celotex*, 477 U.S. at 324, 106 S.Ct. 2548. A nonmoving party cannot avoid summary judgment by relying solely on conclusory allegations that are unsupported by factual data. *See Taylor v. List*, 880 F.2d 1040, 1045 (9th Cir.1989). Likewise, a scintilla of evidence or evidence that is merely colorable or not significantly probative does not present a genuine issue of material fact. *Addisu v. Fred Meyer*, 198 F.3d 1130, 1134 (9th Cir.2000). A dispute is genuine only "if the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986). A fact is "material" only if it "might affect the outcome of the suit under the governing law." *Id.*

Only admissible evidence may be considered in deciding a motion for summary judgment. *Beyene v. Coleman Sec. Servs., Inc.*, 854 F.2d 1179, 1181 (9th Cir.1988). "Credibility determinations, the weighing of the evidence, and the drawing of legitimate inferences from facts are jury functions, not those of a judge ... The evidence of the nonmovant is to be believed, and all justifiable inferences are to be drawn in [its] favor." *Anderson*, 477 U.S. at 255, 106 S.Ct. 2505. "A 'justifiable inference' is not necessarily the most likely inference or the most persuasive inference. Rather, 'an inference as to another material fact may be drawn in favor of the nonmoving party ... if it is 'rational' or 'reasonable.' " *United Steelworkers of Am. v. Phelps Dodge Corp.*, 865 F.2d 1539, 1542 (9th Cir.1989) (internal citation omitted).

IV. PLAINTIFF'S MOTION FOR PARTIAL SUMMARY JUDGMENT ON HIS CLAIMS

A. Declaratory Judgment

Plaintiff seeks a declaratory judgment invalidating two provisions in his employment contract with Priority Sports: (1) the two-year non-compete clause; and (2) the requirement for fourteen days' written notice of termination. (Compl. I. ¶¶ 2, 5). Before reaching the merits, however, the Court addresses Defendants' argument that the issue of the non-compete clause is moot.

1. No Controversy as to Non–Compete Provision

[1][2][3] Where, as here, a plaintiff seeks a declaration pursuant to the Declaratory Judgment Act, 28 U.S.C. § 2201, the district court must first inquire whether there is an actual case or controversy within its jurisdiction. *Principal Life Ins. Co. v. Robinson*, 394 F.3d 665, 669 (9th Cir.2005). "[T]he question in each case is whether the facts alleged, under all the circumstances, show that there is a substantial controversy, between parties having adverse legal interests, of sufficient immediacy and reality ***1028** to warrant the issuance of a declaratory judgment." *Active Sports Lifestyle USA, LLC v. Old Navy, LLC*, No. SACV 12–572 JVS (Ex), 2012 WL 2951924, at *2 (C.D.Cal. July 16, 2012) (internal quotation marks omitted). The burden is on the party seeking declaratory relief to establish the existence of an actual controversy. *Id.* at *2 n. 3.

[4] Here, Defendants claim there is no extant controversy with respect to the non-compete clause because "Priority Sports has made clear to Mintz and CAA that it would not attempt to enforce the two-year non-compete provision at issue." (Def. Opp. at 7); (Dacus Decl. ¶ 8). At the hearing before the Court held on October 29, 2012, defense counsel reassured the Court that Defendants had no intention of seeking to enforce the non-compete clause now or in the future. In response, Plaintiff argues that notwithstanding its proffer, Defendants have refused some requests to stipulate to an order declaring that it will not enforce the non-compete clause. (Horn Decl. ¶ 13). At the hearing, Defendants responded that their refusal was not based on any desire to enforce the non-compete provision, but rather their concerns with the overbreadth of the stipulation. At any rate, there is no evidence that Defendants have attempted, in this or any other litigation, to enforce the non-compete

clause. The Court therefore concludes that Plaintiff has not met its burden of demonstrating an actual controversy with "sufficient immediacy and reality to warrant the issuance of a declaratory judgment." *Active Sports*, 2012 WL 2951924 at *2.

2. No Controversy as to Notice of Termination

[5] Plaintiff next argues that the contractual provision for two-weeks' notice is unenforceable. To be clear, Plaintiff does not take issue with the notice requirement itself. Rather, Plaintiff challenges Priority Sports' supposed position that Plaintiff ***remained*** employed for fourteen days ***after*** his resignation, and thus was barred from competing with Priority Sports during that time. In short, Plaintiff only contends that the two-weeks' notice provision is unenforceable "to the extent Priority Sports asserts it prevented Mintz from competing for clients, including his own clients, ***after*** his resignation." (Reply at 3) (emphasis added).

However, Plaintiff has misconstrued Defendants' position. In their Opposition, Defendants concede that the notice provision "did not prevent Mintz from terminating his employment or from joining CAA; nor did it prevent Mintz from competing fairly with Priority Sports after his termination date." (Opp. at 9). Instead, Defendants only argue that Plaintiff breached the notice provision by failing to give fourteen days' notice of his resignation. Plaintiff cannot conjure an actual controversy by distorting Defendants' position on the notice provision. Given the foregoing, the Court concludes that because Plaintiff and Defendants' positions are not in fact opposed, there is no actual controversy over the effect of the notice provision.

For the reasons above, the Court concludes that there is no litigable controversy with respect to either claim for declaratory relief. Therefore, Plaintiff lacks standing to seek declaratory relief. The Court therefore GRANTS summary judgment for Defendants with respect to the claims for declaratory relief. *See Gospel Missions of America v. City of Los Angeles*, 328 F.3d 548, 553 (9th Cir.2003) ("Even when there has been no cross-motion for summary judgment, a district court may enter summary judgment against a moving party if that party has had a full and fair opportunity to ventilate the issues involved ***1029** in the matter.") (internal quotation marks omitted).

B. Computer Fraud and Abuse Act ("CFAA")

Plaintiff contends that Defendants violated the CFAA by hacking into Plaintiff's Gmail account. (Compl. II ¶¶ 22–25). The CFAA is a federal statute that imposes liability on anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer." 18 U.S.C. § 1030(a)(2). The CFAA also imposes liability on whoever "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value." 18 U.S.C. § 1030(a)(4).

A person who "suffers damage or loss" by reason of a CFAA violation may bring a civil action against the violator under five enumerated circumstances. 18 U.S.C. § 1030(g), (c)(4)(A)(i)(I)–(V). In the present case, only one of these avenues is relevant: Plaintiff must show that his case involves "loss to 1 or more persons during any 1–year period ... aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I). "Loss" is defined as "***any reasonable cost to any victim,*** including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11) (emphasis added).

[6] Defendants do not dispute that Priority Sports violated the terms of either § 1030(a)(2) or (4). (Opp. at 10). Rather, they challenge whether Plaintiff has presented evidence worthy of a directed verdict that he sustained a "loss" in excess of $5,000. Plaintiff has

submitted evidence that he incurred $27,796.25 in attorneys' fees and costs to use the Court's subpoena power to identify Priority Sports as the party that hacked into the Gmail account. (Horn Supp. Decl. (Dkt. 72–1) ¶ 2, Ex. A). The Court concludes, however, that this is insufficient to satisfy the statutory threshold, for two reasons.

First, a "loss" is defined as "any reasonable cost ***to any victim.***" 18 U.S.C. § 1030(e)(11) (emphasis added). It is undisputed, however, that the legal fees in question were paid not by Plaintiff, but by CAA, which is not a victim of this offense. Moreover, Plaintiff has cited no evidence that he will be required to repay CAA in part or in full. Accordingly, there is no basis to conclude that Plaintiff has personally suffered a loss as a result of the offense.[FN3]

> FN3. The Eighth Circuit reached a different conclusion in *United States v. Millot,* 433 F.3d 1057 (8th Cir.2006). The court focused on the language that a plaintiff must show "loss to 1 ***or more persons*** during any 1–year period ... aggregating at least $5,000 in value." *Id.* at 1061–62 (citing 18 U.S.C. § 1030(a)(5)(B)(i) (West 2006)) (emphasis added). However, this approach fails to take account of the fact that "loss" is expressly delimited to the reasonable cost ***to any victim.*** Accordingly, the Court is not persuaded by this non-controlling authority.

Second, even if CAA's involvement does not preclude a finding that Plaintiff suffered a loss, the Court holds that the litigation expenses in this case do not qualify as a "loss" under the CFAA. To be sure, courts in the Ninth Circuit have recognized the general principle that "[c]osts associated with investigating intrusions into a computer network and taking subsequent remedial measures are losses within the meaning of the state." *Kimberlite Corp. v. Does,* No. C08–2147 TEH, 2008 WL 2264485, at *1–2 (N.D.Cal.2008). Careful***1030** examination of these cases, however, reveals that the instant litigation costs do not fall under this precept.

In *Kimberlite,* for instance, an individual hacked into a corporation's computer network and email system. In pursuing a CFAA claim, the plaintiff corporation submitted evidence that its staff "spent over 100 hours investigating the matter and taking steps to repair the Kimberlite email system following the intrusions," and that "the cost of securing the Kimberlite email system and conducting [an] investigation has exceeded $5,000." *Id.* at *2. The court found the alleged loss was enough to state a claim under the CFAA. *See also Multiven, Inc. v. Cisco Systems, Inc.,* 725 F.Supp.2d 887, 895 (N.D.Cal.2010) (awarding summary judgment to plaintiff where it provided evidence that it "expended at least $75,000 investigating the intrusions into their network and restoring the security and integrity of Cisco's proprietary systems"). In both *Kimberlite* and *Multiven,* the expenses were oriented toward investigating the extent of the harm and repairing the harm.

Only in limited circumstances have courts considered the cost of discovering the identity of the offender to be part of the "loss" under the statute. In *SuccessFactors, Inc. v. Softscape, Inc.,* 544 F.Supp.2d 975 (N.D.Cal.2008), one of the plaintiff's competitors hacked into a password-protected area of the plaintiff's website and took several screenshots. *Id.* at 978. The competitor then sent those screenshots to hundreds of the plaintiff's actual or prospective customers in an email titled "SuccessFactors Failures and Problems." *Id.* at 977. The plaintiff brought a CFAA claim, alleging that it had expended more than $5,000 in investigating the extent of the breach and locating the perpetrator's IP address. *Id.* at 981. The Court held that these expenses qualified as a "loss," reasoning that "where the offender has actually accessed protected information, discovering who has that information and what information he or she has is essential to remedying the harm." *Id.* In other words, investigating the perpetrator's identity was only justified to the extent

that it was necessary to remedy the harm.

As an initial matter, the Court recognizes that this case is similar to *SuccessFactors* insofar as the offender here also accessed protected information, namely the employment contract with CAA. However, the instant case is readily distinguishable because the litigation costs in question were not "essential to remedying the harm" of the unauthorized access. In *SuccessFactors,* the relevant "harm" of the unauthorized access was that the plaintiff had no clue whether the hacker might invade the website again or send additional spam emails to the plaintiff's customers. To remove that extant risk, it was necessary for the plaintiff to track down the perpetrator. This kind of harm is conspicuously absent from the instant case. To begin, Plaintiff's own evidence establishes the undisputed fact that, within days of the hacking incident, Plaintiff was already convinced that Priority Sports was responsible for the breach of the Gmail account. (Mintz Decl. ¶ 19); (Ketroser Decl. ¶ 3). Moreover, it is undisputed that within days of the hacking, Plaintiff discovered that a Priority Sports employee, Kenny Zuckerman, had learned of, and disclosed to others, Plaintiff's compensation with CAA. (Mintz. Decl. ¶ 20); (Ketroser Decl. ¶ 2). Thus, by that time, it was pellucid that Priority Sports was responsible for the offense, and that it had accessed Plaintiff's employment contract with CAA. All Plaintiff needed to do to secure his Gmail account—indeed, all he could do—was to change the password and the back-up email address used to retrieve the password. It defies common sense to believe that Plaintiff's subsequent legal efforts to ***1031** confirm Priority Sports' involvement were "essential to remedying the harm" of the unauthorized access. By the time the subpoena motions were filed, the harm had long since run its course. Accordingly, the Court concludes as a matter of law that the litigation costs in this case do not count as a "loss" under the CFAA.

In sum, the undisputed facts establish that Plaintiff fails to satisfy the $5,000 threshold and therefore lacks standing to bring a civil action. The Court therefore GRANTS summary judgment for Defendants on the CFAA claim.

C. Electronic Communications and Privacy Act ("ECPA")

[7] Plaintiff next alleges that Defendants violated the Electronic Communications and Privacy Act ("ECPA") by intentionally intercepting an electronic communication, 18 U.S.C. § 2511(1)(a), intentionally disclosing an electronic communication they knew was obtained through an interception, § 2511(1)(c), and intentionally using the contents of an electronic communication they knew was obtained through an interception, § 2511(1)(d). (Compl. II ¶ 27).

[8] These claims fail as a matter of law because there was no "interception" in this case. For an email to be "intercepted" in violation of the foregoing provisions, "it must be acquired during transmission, not while it is in electronic storage." *Konop v. Hawaiian Airlines, Inc.,* 302 F.3d 868, 878 & n. 6 (9th Cir.2002). The undisputed facts here show that Defendants did not access, disclose, or use any emails that had been acquired during transmission. Rather, the emails Defendants viewed were stored on Gmail.

Plaintiff attempts to skirt this problem by arguing that Priority Sports' conduct violated the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701, et seq., which is located in a separate part of the ECPA. *See Columbia Pictures, Inc. v. Bunnell,* 245 F.R.D. 443, 449–50 (C.D.Cal.2007). Specifically, Plaintiff now suggests that Priority Sports violated the SCA by "intentionally access[ing] without authorization a facility through which an electronic communication service is provided ... and thereby obtain[ing] ... access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a)(1); (Reply at 5).

Plaintiff may not now inject a new theory into the

action at the summary judgment stage. *See Coleman v. Quaker Oats Co.*, 232 F.3d 1271, 1294 (9th Cir.2000). The mere fact that the SCA is also part of the ECPA does not mean it covers the same theory of liability. To state the obvious, section 2701 proscribes unauthorized access to data ***in storage,*** whereas section 2511 prohibits unauthorized access to data ***in transmission.*** These are distinct claims. Nowhere in the complaint does Plaintiff attempt to plead a claim under the SCA.

Because Plaintiff's claim under the ECPA fails as a matter of law, the Court GRANTS summary judgment in favor of Defendants.

D. California Penal Code § 502

Plaintiff alleges that Priority Sports' unauthorized entry into his Gmail account violated California Penal Code § 502. (Compl. II ¶¶ 34–37). That statute imposes liability on whoever "[k]nowingly accesses and without permission ... uses any data, computer, computer system, or computer network in order to ... wrongfully control or obtain money, property, or data." § 502(c)(1).[FN4] In addition, the statute ***1032** permits "the owner or lessee" of the computer or data "who suffers damage or loss by reason of a violation" to bring a civil action. § 502(e)(1). "Section 502 sets no threshold level of damage or loss that must be reached to impart standing to bring suit. Under the plain language of the statute, any amount of damage or loss may be sufficient." *Facebook, Inc. v. Power Ventures, Inc.*, No. C 08–05780 JW, 2010 WL 3291750, at *4 (N.D.Cal.2010) (holding that the fact that plaintiff "expended resources" to stop further violations of § 502 sufficed to establish damages, even if such resources only comprised a few "clicks of a mouse" and some "keystrokes").

> FN4. Plaintiff also alleges that Defendants violated other subsections of § 502, though these claims are superfluous to establish liability in this case. For example, § 502 also imposes liability on any person who takes, copies, or makes use of wrongfully obtained data, § 502(c)(2); or unlawfully accesses or provides a means for accessing any computer, § 502(c)(6)-(7).

[9] Upon review, the Court finds that the undisputed facts show that Priority Sports knowingly and without permission used a computer to wrongfully obtain data, in violation of § 502(c)(1). Specifically, Defendants do not dispute that at the direction of Priority Sport's senior counsel, a Priority Sports employee accessed Plaintiff's Gmail account without permission, and viewed the contents of several emails, including Plaintiff's employment agreement with CAA. (Opp. at 9).

[10] The Court further finds that Plaintiff has experienced sufficient damage to support a private right of action. It is undisputed that after the hacking incident, Plaintiff spent some time restoring his Gmail password and investigating who had hacked the Gmail account. (Mintz Decl. ¶ 19).

In light of the foregoing undisputed facts, the Court concludes that Defendants violated California Penal Code § 502. Accordingly, the Court GRANTS Plaintiff summary judgment on the § 502 claim.

E. Invasion of Privacy

[11] Plaintiff asserts that Priority Sports' unauthorized access to his Gmail account violated his right to privacy under the California Constitution. (Compl. II ¶¶ 47–55). To prevail on this claim, Plaintiff must establish "(1) a legally protected privacy interest, (2) a reasonable expectation of privacy under the circumstances, and (3) a serious invasion of the privacy interest." *Int'l Fed'n Prof'l & Technical Eng'rs, Local 21, AFL–CIO v. Super. Ct.*, 42 Cal.4th 319, 64 Cal.Rptr.3d 693, 165 P.3d 488, 499 (2007).

[12][13] "Whether a legally recognized privacy interest is present in a given case is a question of law to be decided by the court." *Hill v. Nat'l Collegiate*

Athletic Assn., 7 Cal.4th 1, 26 Cal.Rptr.2d 834, 865 P.2d 633, 657 (1994). "Whether plaintiff has a reasonable expectation of privacy in the circumstances and whether defendant's conduct constitutes a serious invasion of privacy are mixed questions of law and fact. If the undisputed material facts show no reasonable expectation of privacy or an insubstantial impact on privacy interests, the question of invasion may be adjudicated as a matter of law." *Id.*

[14][15] If all three of these elements are established, the plaintiff's privacy interest must be balanced against any countervailing interests of the defendant. "Invasion of a privacy interest is not a violation of the state constitutional right to privacy if the invasion is justified by a competing interest." *Id.*, 26 Cal.Rptr.2d 834, 865 P.2d at 655–56. "Conduct alleged to be an invasion of privacy is to be evaluated based on the extent to which it furthers legitimate and important competing interests." *Id.*, 26 Cal.Rptr.2d 834, 865 P.2d at 656.

***1033 1. Legally Protected Privacy Interest**

[16][17][18] Priority Sports does not genuinely dispute that a person has a legally protected privacy interest in his personal financial and employment information. "The protection of one's personal financial affairs ... against compulsory public disclosure is an aspect of the zone of privacy which is protected by the Fourth Amendment and which also falls within that penumbra of constitutional rights into which the government may not intrude absent a showing of compelling need and that the intrusion is not overly broad." *Int'l Fed'n*, 64 Cal.Rptr.3d 693, 165 P.3d at 493. Although the California Supreme Court has recognized that "an individual's expectation of privacy in a salary earned in public employment is significantly less than the privacy expectation regarding income earned in the private sector," *id.*, 64 Cal.Rptr.3d 693, 165 P.3d at 494, this observation reinforces the premise that individuals have a legitimate privacy interest with respect to income earned in the private sector. California courts have similarly recognized an individual's protected privacy interest in his employment personnel file. *See El Dorado Sav. & Loan Ass'n v. Super. Ct.*, 190 Cal.App.3d 342, 235 Cal.Rptr. 303, 304–305 (Ct.App.1987). Here, it is undisputed that Priority Sports used Plaintiff's Gmail account to view information about the terms of Plaintiff's employment with CAA, including his compensation. This clearly implicated Plaintiff's legally protected interest in the privacy of his employment and financial affairs.

2. Expectation of Privacy

[19] Plaintiff has presented evidence that he had a reasonable expectation of privacy in his personal emails. It is undisputed that the hacked Gmail account was a web-based, personal email account under the address, amintz 31@ gmail. com. (DUF 7–12). Plaintiff attested in his declaration that he has been the sole account holder since he opened the account. (Mintz Decl. ¶ 18). He further averred that he has "accessed the account through the website www. gmail. com and [has] used it for personal matters." (*Id.*). He had a separate business email address, aaronm@ prioritysports. biz, which he used for business matters. (*Id.*). He only forwarded email from the business account to the personal account when the email itself concerned personal matters (e.g., medical issues), or if he needed to print a document away from the office where he could not access the business account. (*Id.*). Plaintiff's Gmail account was password protected at all times, and he has never authorized any Priority Sports employees to access it. (*Id.*). Based on the foregoing, a reasonable jury could only find that Plaintiff had an expectation of privacy in this personal email account.

Defendants argue that Plaintiff engaged in conduct that belied his expectation of privacy, but none of these contentions have merit. First, Defendants suggest that it was Plaintiff, not Priority Sports, who first divulged the terms of the CAA agreement to a third party named Josh Ketroser. (Opp. at 13). This mischaracterizes Ketroser's testimony. In fact, Ketroser stated that after Plaintiff's resignation, Kenny Zuck-

erman, an employee of Priority Sports, first disclosed to Ketroser that he had accessed Plaintiff's email account and discovered that his salary at CAA would be less than at Priority Sports. (Ketroser Decl. ¶ 2). It was only afterward that Ketroser contacted Plaintiff, who confirmed the salary figures. (*Id.* ¶ 3).

Second, Defendants argue, without citing specific evidence, that Plaintiff's girlfriend, Jenna Manos, had access to Plaintiff's Gmail account. However, Plaintiff testified that he gave Manos access to his temporary password so that she could help ***1034** him investigate who had hacked his Gmail account. (Mintz Decl. ¶ 19). Defendants cite no specific evidence that Manos had always had access to the Gmail account. Therefore, this does not create a triable issue as to whether Plaintiff had an expectation of privacy in the Gmail account.

Third, Defendants contend that because Plaintiff disclosed to CAA the terms of his employment agreement with Priority Sports, he must not, as a general matter, treat any of his employment agreements as confidential. This argument is frivolous. Plaintiff's decision to disclose his existing employment terms in the course of negotiations with CAA does not constitute evidence that he relinquished any expectation of privacy in his separate employment agreement with CAA. If anything, Plaintiff's conduct is consistent with an expectation that absent his voluntary disclosure, the terms of his employment with Priority Sports would have remained confidential.

In sum, Defendants have failed to point to specific facts raising a triable issue of whether Plaintiff had a reasonable expectation of privacy. The Court therefore turns to whether Plaintiff has suffered a substantial invasion of his privacy.

3. Serious Invasion of Privacy Interest

[20] "Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right."*Hill,* 26 Cal.Rptr.2d 834, 865 P.2d at 655. Here, Priority Sports' employee, Ames, admitted in his deposition that (1) he purposely obtained a temporary password to Plaintiff's Gmail account without permission, (2) he opened two to three emails that had been forwarded from Plaintiff's Priority Sports email account; (3) he opened an additional three to four***personal*** emails that had ***not*** come from Plaintiff's business account; (4) that one of these personal emails related to Plaintiff's employment agreement with CAA; and (5) he then viewed the CAA employment agreement itself. (DUF 7–12).

[21] Based on this evidence, it is clear that Ames did not accidentally stumble into Plaintiff's zone of privacy. *Cf. Hernandez v. Hillsides, Inc.,* 47 Cal.4th 272, 97 Cal.Rptr.3d 274, 211 P.3d 1063, 1079 (2009) ("[N]o cause of action will lie for accidental, misguided, or excusable acts of overstepping upon legitimate privacy rights."). Instead, Ames deliberately accessed Plaintiff's Gmail account without permission, opened several emails, and even read their contents, including the CAA agreement. Indeed, this conduct is so serious and offensive that the California legislature subjects the perpetrator to criminal liability under California Penal Code § 502. Faced with the foregoing, no reasonable jury could find that the invasion was not an egregious breach of social norms.

Rather than citing facts to dispute the seriousness of the invasion, Defendants baldly assert that the intrusion was "de minimis" because it "stems from a review of Mintz's agreement with CAA, nothing more." (Opp. 13). This contention lacks merit. As discussed above, Ames first had to hack into Plaintiff's Gmail account and open several other emails before he read the CAA agreement. This conduct was illegal under California law. Therefore, Defendants have failed to create a triable issue that the invasion was not serious.

4. Competing Interests

Defendants have not posited, and the Court is unaware of any legitimate competing interests that would justify an employer to obtain unauthorized access to an employee's personal, password-protected email account. The balance therefore weighs decisively in favor of Plaintiff.

***1035** Based on the foregoing analysis, the Court concludes that Defendants have failed to adduce specific facts to controvert the evidence supporting the serious invasion that took place in this case. Accordingly, the Court GRANTS Plaintiff summary judgment on the invasion of privacy claim.

F. Unfair Competition Law

[22] Plaintiff alleges that by virtue of the aforementioned claims, Defendants have engaged in "unlawful business acts or practices" in violation of California's UCL. (Compl. II ¶¶ 67–75). The statute proscribes any business act or practice forbidden by another law. *Walker v. Countrywide Home Loans, Inc.*, 98 Cal.App.4th 1158, 1169, 121 Cal.Rptr.2d 79 (2002). However, following the passage of Proposition 64, a private plaintiff has standing to sue under the UCL only if he "has suffered injury in fact and has lost money or property as a result of such unfair competition." *Californians for Disability Rights v. Mervyn's, LLC*, 39 Cal.4th 223, 46 Cal.Rptr.3d 57, 138 P.3d 207, 209 (2006) (internal quotation marks omitted). "The plain import of this is that a plaintiff now must demonstrate some form of economic injury." *Kwikset Corp. v. Superior Court*, 51 Cal.4th 310, 120 Cal.Rptr.3d 741, 246 P.3d 877, 885 (2011).

[23] Even if Plaintiff has suffered some injury, he has failed to carry his initial burden to show that he lost any money or property as a result of violations of other laws. "Numerous courts have held that a plaintiff's 'personal information' does not constitute money or property under the UCL." *In re iPhone Application Litig.*, No. 11–MD–02250–LHK, 2011 WL 4403963, at *14 (N.D.Cal. Sept. 20, 2011). Accordingly, the Court DENIES Plaintiff's Motion for Summary Judgment on the UCL claim.[FN5]

FN5. The Court would have gone further and granted summary judgment in favor of Defendants, but for the fact that Plaintiff's claims for defamation and economic interference remain outstanding. Because the fact-finder may decide at trial that the defamation and intentional interference, if any, resulted in economic injury, it is possible that these claims would form the predicate acts of Plaintiff's UCL claim. The Court therefore declines to grant summary judgment for Defendants on the UCL claim.

V. PLAINTIFF AND CAA'S MOTION FOR SUMMARY JUDGMENT AS TO PRIORITY SPORTS' COUNTERCLAIMS[FN6]

FN6. This section overlaps with Defendants' Cross–Motion for Partial Summary Judgment on its claims for breach of contract and breach of the duty of loyalty.

A. Breach of Contract (Against Plaintiff)

In its counterclaim, Priority Sports alleges that Plaintiff breached his employment contract by, inter alia, (1) working for CAA prior to his resignation; (2) soliciting players on CAA's behalf prior to his resignation; (3) misappropriating Priority Sports' trade secret and confidential information and sharing it with CAA before and after his resignation; (4) failing to provide fourteen days' written notice; and (5) failing to return company property, i.e. conversion. (Counterclaim ¶ 67). Because the Court concludes in separate sections below that the misappropriation and conversion claims fail as a matter of law, they likewise cannot support a breach of contract claim here. The Court therefore proceeds to address whether Priority Sports has raised any triable issues as to the remaining grounds for breach of contract.

[24] A claim for breach of contract has three essential elements: "(1) the existence of the contract, (2) plaintiff's performance or excuse for nonperformance, ***1036** (3) defendant's breach, and (4) the resulting damages to the plaintiff." *Oasis West Realty, LLC v. Goldman*, 51 Cal.4th 811, 124 Cal.Rptr.3d 256, 250 P.3d 1115, 1121 (2011).

[25] Plaintiff moves for summary judgment on the ground that Priority Sport has failed to raise a triable issue that it suffered damages as a result of any breach by Plaintiff. For example, Plaintiff concedes that there is evidence that, at some point before or after his resignation, he solicited the personal agent of NBA player Taj Gibson. Even assuming the conversation took place before Plaintiff's resignation, it is undisputed that Gibson did not leave Priority Sports to follow Plaintiff to CAA. (DUF 23); (Mintz Decl. ¶ 35). Accordingly, no jury could find that this harmed Priority Sports.

To attempt to stave off summary judgment, Priority Sports cites a different example of Plaintiff's alleged misconduct. Priority Sports alleges that Plaintiff "admitted that he communicated with at least two recruits while at Priority Sports, Mike Scott and Terrence Ross, did not provide updated information to Priority Sports, and instead signed their deals at CAA." (Opp. at 16). This bare allegation fails to raise a triable issue for several reasons. To begin, Priority Sports entirely neglects to cite the relevant facts in the record that support this assertion.[FN7] Nor has Priority Sports directed the Court to any shred of evidence that Scott and Ross are now clients with CAA. Furthermore, the only place in the record any ostensible support is found is in the declaration of Mark Bartelstein. He only averred, however, that Plaintiff failed to inform him of "communications" or "contacts" with Scott, Ross, and Sacre prior to Plaintiff's resignation. Even crediting this testimony, which lacks foundation, there is no evidence that Plaintiff's "communications" with these players included solicitations to join CAA. To make this assumption would constitute mere speculation. *Juan H. v. Allen*, 408 F.3d 1262, 1277 (9th Cir.2005) ("A 'reasonable' inference is one that is supported by a chain of logic, rather than, as in this case, mere speculation dressed up in the guise of evidence."). For all the reasons above, these allegations are insufficient to create a triable issue.

FN7. Priority Sports cites "Additional Material Facts" 47 and 48, but these cited parts of the record do not support the allegations concerning Ross and Scott. This lack of diligence is reason enough to disregard these allegations. *Carmen v. San Francisco Unified School District*, 237 F.3d 1026, 1031 (9th Cir.2001) ("The district court need not examine the entire file for evidence establishing a genuine issue of fact, where the evidence is not set forth in the opposing papers with adequate references so that it could conveniently be found.").

[26] Priority Sports likewise cannot establish damage resulting from Plaintiff's failure to give fourteen days' notice. Priority Sports contends that the lack of notice "deprived Priority Sports of the opportunity to reach out to those of its clients who had worked with client-service teams that included Mintz and to secure its relationships with those clients before Mintz's departure was a *fait accompli*." (Opp. at 16). The sole support for this assertion is Bartelstein's declaration, in which he claims that because of the lack of notice, he was unable to contact a client until five days after Plaintiff's resignation. (Bartelstein Decl. ¶ 7). But Bartelstein also concedes that the client remained with Priority Sports. (*Id.*). Therefore, there is no basis to conclude Priority Sports was damaged. Moreover, Bartelstein's deposition testimony belies the contention that the lack of notice prevented Priority Sports from calling its clients. When asked, "Didn't you call all of those players?" Bartelstein replied, "I did." (Horn ***1037** Decl. (Dkt. 61), Ex. A at 301:9–11). Finally, Priority Sports fails to identify a

single client that it lost as result of Plaintiff's failure to give notice. Based on this deficient showing, the Court concludes that no rational fact-finder could conclude that Plaintiff's failure to give notice damaged Priority Sports.

In review, Priority Sports has failed to create a triable issue that it suffered damages as a result of the alleged breach of contract. Accordingly, the Court GRANTS Plaintiff summary judgment on the breach of contract counterclaim.

B. Breach of Implied Covenant of Good Faith and Fair Dealing (Against Plaintiff)

[27] Where "allegations of breach of the covenant of good faith do not go beyond the statement of a mere contract breach and, relying on the same alleged acts, simply seek the same damages or other relief already claimed in a companion contract cause of action, they may be disregarded as superfluous as no additional claim is actually stated." *Bionghi v. Metropolitan Water Dist. of So. California*, 70 Cal.App.4th 1358, 83 Cal.Rptr.2d 388 (Ct.App.1999).

In reviewing Priority Sports' Counterclaim, it clearly relies on the same predicate acts that undergird the breach of contract claim. (Counterclaim ¶¶ 71–74). Priority Sports responds in its papers by raising various new theories of liability not raised in the Counterclaim, but these may not be deployed at the last minute to avoid summary judgment. *See Coleman*, 232 F.3d at 1294. Thus, the Court GRANTS Plaintiff summary judgment on the breach of implied covenant counterclaim.

C. Breach of the Duty of Loyalty (Against Plaintiff)

[28] Priority Sports next alleges that Plaintiff breached his duty of loyalty to Priority Sports. To establish this claim, Priority Sports must demonstrate: "(1) the existence of a relationship giving rise to a duty of loyalty; (2) one or more breaches of that duty; and (3) damage proximately caused by that breach." *Huong Que, Inc. v. Luu*, 150 Cal.App.4th 400, 58 Cal.Rptr.3d 527, 535 (Ct.App.2007).

Preliminarily, the Court notes that this claim is based in large part on the same factual allegations of misconduct discussed in the section above. (Counterclaim ¶ 77). Because the foregoing facts do not create a triable issue of breach of contract, neither can they give rise to a breach of the duty of loyalty. *Nygard, Inc. v. Uusi–Kerttula*, 159 Cal.App.4th 1027, 72 Cal.Rptr.3d 210, 224 (Ct.App.2008) (because defendant did not breach his employment contract, the court "necessarily" concluded that he did not breach the duty of loyalty).

The Court recognizes, however, that Priority Sports also bases its duty of loyalty claim on other factual allegations not discussed above. For example, the Counterclaim alleges that Plaintiff planned his transition to CAA while he was still employed by Priority Sports. (Counterclaim ¶¶ 77(e)-(f)). Thus, in its Opposition, Priority Sports points to facts that supposedly establish a pattern of disloyal conduct: (1) Plaintiff and CAA agreed that CAA would pay for Plaintiff's representation in connection with his future employment with CAA; (2) Plaintiff and CAA entered into a joint defense agreement related to the instant litigation; and (3) Plaintiff met with CAA's attorneys once he decided he would resign from Priority Sports. (Def. St. Uncontroverted Facts II (Dkt. 56–1) ¶¶ 16–18).

[29][30][31] Even if these facts are true, they do not create a triable issue for two reasons. First, under California law, an employee does not breach his duty of loyalty merely by preparing to compete with his employer. ***1038***Mamou v. Trendwest Resorts, Inc.*, 165 Cal.App.4th 686, 81 Cal.Rptr.3d 406, 433 (Ct.App.2008). Thus, courts have held that an employee may set up a competing organization without breaching the duty of loyalty. *Id.* at 433–34. While some preparation is permitted, "California law does not authorize an employee to transfer his loyalty to a

competitor." *Fowler v. Varian Assoc., Inc.*, 196 Cal.App.3d 34, 241 Cal.Rptr. 539, 543 (Ct.App.1987). Here, Plaintiff's interactions with CAA and its attorneys were made in preparation for his future employment with CAA. Without more, however, the facts presented do not reasonably support an inference that Plaintiff had transferred his loyalty to CAA before his resignation.

[32] Second, and in any event, Priority Sports has presented no facts that describe how it was harmed by Plaintiff's preparatory steps. It fails to direct the Court to any evidence, for example, that Plaintiff's plan-making resulted in the loss of a client. Nor has Priority Sports pointed to evidence of how it may have been disadvantaged in this litigation by virtue of Plaintiff's anticipatory steps. Because there is no triable issue of breach or of damages, the Court GRANTS Plaintiff summary judgment on the duty of loyalty counterclaim.

D. Misappropriation of Trade Secrets (Against Counterdefendants)

[33][34] Priority Sport's Fourth Counterclaim is for misappropriation of trade secrets in violation of California's Uniform Trade Secrets Act ("CUTSA"), Cal. Civ.Code § 3426.1. This claim has three core elements: "(1) the plaintiff owned a trade secret, (2) the defendant acquired, disclosed, or used the plaintiff's trade secret through improper means, and (3) the defendant's actions damaged the plaintiff." *Cytodyn, Inc. v. Amerimmune Pharm., Inc.*, 160 Cal.App.4th 288, 72 Cal.Rptr.3d 600, 607 (Ct.App.2008); Cal. Civ.Code 3426.1(b). The CUTSA defines a "trade secret" as:

> [I]nformation, including a formula, pattern, compilation, program, device, method, technique or process that: (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Cal. Civ.Code § 3426.1(d). Plaintiff argues, inter alia, that Priority Sports has failed to offer evidence of any specific instance of misappropriation. The Court agrees.

Priority Sports' Opposition is utterly devoid of evidence that Plaintiff or CAA misappropriated any trade secrets belonging to Priority Sports. Priority Sports argues that Plaintiff "concedes" to using Priority Sports' client lists to contact unidentified "players" via Skype on behalf of CAA. (Opp. 15:10–13, 19:7–9 (citing AMF 47, 55)). The cited evidence, however, comprises statements by Bartelstein, not by Plaintiff. Moreover, none of Bartelstein's statements mention any misappropriation by Plaintiff or CAA. (Bartelstein Decl. ¶¶ 6–7, 13–14). Because Priority Sports has failed to discharge its burden under Rule 56, the Court GRANTS Plaintiff and CAA summary judgment on the misappropriation counterclaim.

E. Intentional Interference with Contractual Relations (Against CAA)

[35][36] Priority Sport asserts that CAA induced Plaintiff to breach his employment contract. (Counterclaim ¶ 93). In the usual case, to prove intentional interference with contractual relations, a plaintiff must demonstrate:

> ***1039** (1) a valid contract between plaintiff and a third party; (2) defendant's knowledge of this contract; (3) defendant's intentional acts designed to induce a breach or disruption of the contractual relationship; (4) actual breach or disruption of the contractual relationship; and (5) resulting damage.

Pac. Gas & Elec. Co. v. Bear Stearns & Co., 50 Cal.3d 1118, 270 Cal.Rptr. 1, 791 P.2d 587, 589–90 (1990). However, California affords greater solicitude to interfering conduct in the context of at-will em-

ployment:

> [T]o recover for a defendant's interference with an at-will employment relation, a plaintiff must plead and prove that the defendant engaged in an independently wrongful act—i.e., an act proscribed by some constitutional, statutory, regulatory, common law, or other determinable legal standard—that induced an at-will employee to leave the plaintiff.

Reeves v. Hanlon, 33 Cal.4th 1140, 17 Cal.Rptr.3d 289, 95 P.3d 513, 520 (2004) (internal citation and quotation marks omitted).

[37] Priority Sports has failed to present any evidence that CAA committed any independently wrongful act to induce Plaintiff to breach or disrupt its at-will employment contract with Priority Sports. This conclusion is bolstered by the Court's grant of summary judgment for CAA on the misappropriation counterclaim. Accordingly, the Court GRANTS CAA summary judgment as to the interference with contractual relations counterclaim.

F. Intentional Interference with Present and Prospective Economic Advantage and Business Relationships (Against Plaintiff and CAA)

Priority Sports alleges that (1) CAA interfered with Priority Sports' business relationship with Plaintiff; and (2) Plaintiff and CAA interfered with Priority Sports' business relationships with NBA players. (Counterclaim ¶¶ 100–101).

[38] The elements of a claim for intentional interference with prospective economic advantage mirror those for intentional interference with an at-will employment contract, including the requirement that the plaintiff establish that the defendant engaged in an "independently wrongful act," that is, "if it is proscribed by some constitutional, statutory, regulatory, common law, or other determinable legal standard." *Korea Supply Co. v. Lockheed Martin Corp.,* 29 Cal.4th 1134, 131 Cal.Rptr.2d 29, 63 P.3d 937, 953–54 (2003).

The Court has already determined that no jury could find that (1) Plaintiff breached the employment contract, the implied covenant, or his duty of loyalty; or that (2) Plaintiff or CAA misappropriated any of Priority Sports' trade secrets; or that (3) CAA intentionally interfered with Priority Sports' contractual relations with Plaintiff. Apart from this, Priority Sports provides no evidence that either Plaintiff or CAA has engaged in any other independently wrongful conduct. Accordingly, the Court GRANTS Counterdefendants summary judgment as to this counterclaim.

G. Conversion (Against Plaintiff)

Defendants assert that Plaintiff removed and retained without permission property belonging to Priority Sports, including two boxes of documents, a laptop computer, and cell phone. (Counterclaim ¶ 105). Priority Sports has since conceded, however, that Plaintiff has returned the laptop and the boxes of documents. (Counterclaim ¶ 84); (Opp. at 21). Thus, the only question is whether Plaintiff's failure to return the cell phone constitutes conversion.

***1040** [39] Conversion has three elements under California Law: (1) ownership or right to possession of property; (2) wrongful disposition of the property right; and (3) damages. *G.S. Rasmussen & Assoc., Inc. v. Kalitta Flying Services, Inc.,* 958 F.2d 896, 906 (9th Cir.1992). Plaintiff asserts that the cell phone belongs to him, and that he has turned over to Priority Sports any telephone numbers and text messages on the device. (UF 57). Plaintiff further argues that Priority Sports cannot show it has been damaged.

[40] Priority Sports claims ownership on the ground that "Mintz recently admitted in deposition that he still has possession of his company Blackberry and that he is not willing to return it to Priority Sports." (Opp. at 21:13–15 (citing AMF 38)). The

cited evidence, however, states to the contrary that "Priority Sports and Mr. Mintz dispute ownership of the Blackberry he used while employed by Priority Sports." (Horn Decl. ¶ 15). This is not the first time in this Order that the Court has exposed clear misstatement of evidence by counsel for Priority Sports. Counsel are warned that further errors of such an egregious nature will be construed by the Court as indicative of bad faith, and may be grounds for sanctions. At any rate, this error serves to highlight Priority Sports' lack of evidence that it owns the cell phone in question. The Court GRANTS Plaintiff summary judgment as to the conversion claim.

H. California Penal Code § 502 (Against Plaintiff)

Priority Sports initially claimed that Plaintiff accessed its computers without permission and copied or deleted data in violation of California Penal Code § 502(c)(1), (2), (3), (6), (7). (Counterclaim ¶¶ 110, 111, 113). Plaintiff contends, however, that the evidence refutes this allegation. Specifically, when Bartelstein, Priority Sport's "Person Most Knowledgeable," was asked, "You can't identify any files that Mr. Mintz copied or deleted from Priority Sports, correct, you sitting here today cannot?" Bartelstein responded, "Correct." (Bartelstein Depo. at 147:5–16).

In response, Priority Sports shifts theories, arguing that Plaintiff violated § 502 by wrongfully accessing Priority Sports' confidential information and forwarding it to his Gmail account. This argument fails for two reasons. First, Priority Sports cite no supportive facts in their papers. "Rule 56(e) requires that the adverse party's response, not just the adverse party's various other papers, set forth specific facts establishing a genuine issue." *Carmen*, 237 F.3d at 1031.

[41][42] Second, Priority Sports concedes the absence of evidence showing that Priority Sports was damaged by the email forwarding. Specifically, Priority Sports admits that "additional discovery is needed to determine whether and to what extent Mintz's unauthorized access to Priority Sports' computers caused 'damages' of the type that Section 502 was designed to protect." (Opp. at 25 n. 3). As a threshold matter, a party seeking further discovery under Rule 56(d)(2) must show that "(1) it has set forth in affidavit form the specific facts it hopes to elicit from further discovery; (2) the facts sought exist; and (3) the sought-after facts are essential to oppose summary judgment." *Family Home & Fin. Ctr., Inc. v. Fed. Home Loan Mortg. Corp.*, 525 F.3d 822, 827 (9th Cir.2008). Priority Sports has failed to file such an affidavit. In any event, the Court finds that Priority Sports has had ample opportunity to pursue discovery on the issue of damages. Accordingly, the Court proceeds to summary judgment. *Id.* Because Priority Sports has failed to show any evidence of damages, the Court GRANTS ***1041** Plaintiff summary judgment on the § 502 claim.

I. Defamation and Trade Libel (Against Plaintiff)

Priority Sports alleges that Plaintiff uttered several false and defamatory statements about Priority Sports to third parties that have damaged Priority Sports. It further alleges that Plaintiff made false statements disparaging the quality of Priority Sports' property, goods, and/or services, which has damaged Priority Sports. (Counterclaim ¶¶ 119–22, 127–29). Specifically, Priority Sports asserts "on information and belief" that Plaintiff told an industry blogger that another employee was leaving Priority Sports. (Horn Decl. ¶ 16, Ex. L, Response to Interrogatory 1). In addition, Plaintiff allegedly made various statements to certain NBA players or their associates, conveying that: (1) there would be a "mass exodus" of players from Priority Sports; (2) Priority Sports "was going to fall apart" because of Plaintiff's departure; (3) Bartelstein was "just a figurehead" and Plaintiff "did all the work;" (4) Bartelstein did not have certain players "best interests" in mind; (5) Bartelstein favored other players over the percipient players. (DUF 63).

[43] Plaintiff contends that Priority Sports has not produced evidence that Plaintiff made these state-

ments, and that in any event, the statements are inadmissible hearsay and non-actionable opinions. In response, Priority Sports proffers that it "will prove at trial" that Plaintiff made these statements. Priority Sports misunderstands the purpose of summary judgment: now is the time to produce evidence. Priority Sports has failed to identify any testimony from third parties attesting that Plaintiff made any of the alleged statements. A nonmoving party cannot avoid summary judgment by relying solely on conclusory allegations that are unsupported by factual data. *Taylor*, 880 F.2d at 1045.

Priority Sports blames its lack of evidence on CAA for its failure to produce certain NBA players for depositions. Accordingly, Priority Sports requests a continuance pursuant to Rule 56(d)(2). (Opp. at 23–24). However, as already explained, a party seeking a continuance pursuant to Rule 56(d)(2) must show that "(1) it has set forth in affidavit form the specific facts it hopes to elicit from further discovery; (2) the facts sought exist; and (3) the sought-after facts are essential to oppose summary judgment." *Family Home*, 525 F.3d at 827.

[44] Priority Sports has not satisfied the requirements of Rule 56(d). Its request for a continuance "did not identify the specific facts that further discovery would have revealed or explain why those facts would have precluded summary judgment." *Tatum v. City and Cnty. of San Francisco*, 441 F.3d 1090, 1100 (9th Cir.2006). In a declaration supporting Priority Sports' Opposition, defense counsel stated that he was informed that "counsel for Priority Sports identified to CAA players it believed overheard defamatory statements and CAA's counsel represented that it would accept service for those players." (Dacus Decl. ¶ 9). The declaration does not, however, refer to any specific facts that the players would establish, or explain why their testimony was "essential to justify" Priority Sport's opposition. Fed.R.Civ.P. 56(d). The declaration does not indicate that deferring the resolution of Plaintiff's Motion for Summary Judgment until these players have been deposed would have allowed Priority Sports to supply evidence creating a triable issue that Plaintiff made defamatory remarks that caused damaged. Absent a showing pursuant to Rule 56(d), the Court denies Priority Sports' request for a continuance.

***1042** Because Priority Sports has failed to create a triable issue that Plaintiff made any defamatory or libelous statements, the Court GRANTS Plaintiff summary judgment on the defamation and trade libel claims.

J. Conspiracy (Against Counterdefendants)

[45][46] Priority Sports alleges that Plaintiff and CAA conspired to commit the alleged wrongful acts described in the preceding sections, including the breach of contract, breach of duty of loyalty, and misappropriation. (Counterclaim ¶ 133). "Standing alone, a conspiracy does no harm and engenders no tort liability. It must be activated by the commission of an actual tort. A civil conspiracy, however atrocious, does not give rise to a cause of action unless a civil wrong has been committed resulting in damage." *Applied Equipment Corp. v. Litton Saudi Arabia Ltd.*, 7 Cal.4th 503, 28 Cal.Rptr.2d 475, 869 P.2d 454, 457 (1994) (internal quotation marks omitted).

Counterdefendants argue that the conspiracy claim cannot survive summary judgment because Priority Sports has failed to raise a triable issue as to any predicate tortious acts. Priority Sports responds with the naked assertion that "there is substantial evidence that Mintz and CAA conspired with each other to inflict severe harm on Priority Sports, both financially and to its reputation, and Priority Sports is entitled to present such evidence in support of its claims at trial." (Opp. at 24). This mere conclusion is insufficient to raise a triable issue of fact. Because there is no evidence of any predicate wrongful acts, the Court GRANTS Counterdefendants summary judgment on the conspiracy claim.

K. Unfair Competition Law (Against Counterdefendants)

[47] Finally, Priority Sports alleges that it was damaged by Counterdefendants' "unlawful, unfair, or fraudulent business practices." (Counterclaim ¶ 139). "By proscribing 'any unlawful' business practice, section 17200 borrows violations of other laws and treats them as unlawful practices that the unfair competition law makes independently actionable." *Cel–Tech Comms. Inc. v. L.A. Cellular Tel. Co.*, 20 Cal.4th 163, 83 Cal.Rptr.2d 548, 973 P.2d 527, 539–40 (1999). "However, the law does more than just borrow.... Because Business and Professions Code section 17200 is written in the disjunctive, it establishes three varieties of unfair competition—acts or practices which are unlawful, or unfair, or fraudulent. In other words, a practice is prohibited as 'unfair' or 'deceptive' even if not 'unlawful' and vice versa." *Id.*, 83 Cal.Rptr.2d 548, 973 P.2d at 540.

Here, Plaintiff argues that the UCL claim fails because neither Plaintiff nor CAA violated an underlying, predicate law. In response, Priority Sports rests on its papers, maintaining that it "has obtained substantial evidence that Mintz and CAA engaged in numerous unfair and unlawful acts that support their claim for violation of the UCL." (Opp. at 25). The Court has already determined, however, that the evidence presented does not create any triable issue that Counterdefendants are liable for any unlawful act. Moreover, Priority Sports fails to identify any evidence creating any triable issue that Counterdefendants' behavior was unfair or fraudulent within the meaning of the UCL. Because Priority Sports failed to carry its burden under Rule 56(e), the Court GRANTS Counterdefendants summary judgment as to the UCL claim.

***1043 VI. CONCLUSION**

For the reasons above, Plaintiff's Motion for Summary Judgment on its own claims is GRANTED with respect to the claims for violation of California Penal Code § 502 and invasion of privacy, but DENIED with respect to the claim under the UCL. Further, the Court GRANTS summary judgment in favor of Defendants on Plaintiff's claims for declaratory relief, violation of the CFAA, and violation of the ECPA. Counterdefendants' Motion for Summary Judgment as to Defendants' counterclaims is GRANTED as to every claim. Defendants' Motion for Partial Summary Judgment on its breach of contract and breach of duty of loyalty claims is DENIED as moot. In short, the only causes of action that remain to be tried are Plaintiff's claims for defamation, interference with prospective economic relations, and violation of the UCL.

C.D.Cal.,2012.
Mintz v. Mark Bartelstein and Associates Inc.
906 F.Supp.2d 1017

END OF DOCUMENT

949 F.Supp.2d 748
United States District Court,
N.D. Ohio,
Western Division.

Sandi **LAZETTE**, Plaintiff
v.
Chris **KULMATYCKI**, et al., Defendant.

Case No. 3:12CV2416. | June 5, 2013.

Synopsis

Background: Former employee brought action against former employer and supervisor, alleging violations of the Stored Communications Act (SCA), the Omnibus Crime Control and Safe Streets Act, and Ohio law for invasion of privacy and intentional infliction of emotional distress (IIED). Defendants' moved to dismiss.

Holdings: The District Court, James G. Carr, Senior Judge, held that:

[1] SCA applied;

[2] server that stored personal e-mails, rather than smartphone that accessed those e-mails, was a facility under SCA;

[3] employee negligently leaving application to access her personal e-mail on employer-issued smartphone was not consent;

[4] that employer informed employee that her e-mail might be monitored was not implied consent;

[5] e-mails that employee opened but did not delete were not in electronic storage;

[6] allegations were sufficient to state a claim under SCA; and

[7] allegations were sufficient to state a claim under Ohio law for intrusion into seclusion as an invasion of privacy.

Motion granted in part and denied in part.

West Headnotes (16)

[1] Telecommunications
Computer communications

Prohibitions of Stored Communications Act (SCA) applied in former employee's action against former employer and supervisor, alleging violations of the SCA in supervisor reading employee's personal e-mail over 18 months on company-issued smartphone that employee returned upon leaving employer; SCA applied to persons or entities and prohibited intentionally accessing electronic data without or in excess of authorization. 18 U.S.C.A. § 2701.

Cases that cite this headnote

[2] Telecommunications
Computer communications

Use of a password is not an element of a claim under the Stored Communications Act (SCA). 18 U.S.C.A. § 2701.

Cases that cite this headnote

[3] Telecommunications
Computer communications

That supervisor used company-owned smartphone, which former employee had used previously and returned upon leaving employer, to access employee's personal e-mail on phone did not mean he acted with authorization when he accessed e-mails, for purposes of employee's Stored Communications Act (SCA) claim against supervisor and employer. 18 U.S.C.A. § 2701.

Cases that cite this headnote

[4] Telecommunications
Computer communications

Server that stored personal e-mails, rather than smartphone that accessed those e-mails, was a "facility" under Stored Communications Act (SCA), and therefore, supervisor's authorization to use company-issued smartphone, which

had been returned by employee upon leaving employer, did not preclude employee's SCA claim alleging violations of SCA in supervisor accessing her personal e-mails for 18 months without authorization. 18 U.S.C.A. § 2701(a)(1).

Cases that cite this headnote

[5] Telecommunications

Computer communications

The Stored Communications Act (SCA) does not require one who accesses a service provider without authorization also to have done something to the equipment to facilitate his access. 18 U.S.C.A. § 2701.

Cases that cite this headnote

[6] Telecommunications

Computer communications

Employee negligently leaving application to access her personal e-mail on employer-issued smartphone she returned upon leaving employer was not consent for supervisor to read all her e-mails over 18 months, as required for her Stored Communications Act (SCA) claim against employer and supervisor. 18 U.S.C.A. § 2701(a)(1).

Cases that cite this headnote

[7] Telecommunications

Computer communications

Consent for access, for purposes of the Stored Communications Act (SCA), need not be explicit, it can also be implied; negligence is, however, not the same as approval, much less authorization. 18 U.S.C.A. § 2701(a)(1).

1 Cases that cite this headnote

[8] Telecommunications

Computer communications

That employer informed employee that her e-mail might be monitored on her employer-issued smartphone did not provide implied consent for supervisor to read all her personal e-mail over 18 months after employee returned smartphone upon leaving employer, as required for her Stored Communications Act (SCA) claims against employer and supervisor. 18 U.S.C.A. § 2701(a)(1).

Cases that cite this headnote

[9] Telecommunications

Computer communications

E-mails that former employee opened but did not delete were not in electronic storage under the Stored Communications Act (SCA) when supervisor accessed them on employer-issued smartphone, which employee had returned previously when leaving employer, and therefore, supervisor's access of such e-mails did not violate the SCA. 18 U.S.C.A. § 2701(a).

4 Cases that cite this headnote

[10] Telecommunications

Computer communications

Former employee's allegations that she returned employer-issued smartphone upon leaving employment, that supervisor accessed her personal e-mail on smartphone over 18 months, and that he opened some of e-mails before employee did were sufficient to state a claim under the Stored Communications Act (SCA) against supervisor and employer. 18 U.S.C.A. § 2701(a).

Cases that cite this headnote

[11] Telecommunications

Computer communications

Former employee's allegations that she returned employer-issued smartphone upon leaving employment, that supervisor accessed her personal e-mail on smartphone over 18 months, that he opened some of e-mails before employee did, and that supervisor's conduct was within scope of his employment and in furtherance of employer's interest were sufficient to state claim for vicarious liability for employee's Stored Communications Act (SCA) claims against employer. 18 U.S.C.A. § 2701(a).

Cases that cite this headnote

[12] Telecommunications

Computer communications

Supervisor did not intercept former employee's personal e-mails in accessing e-mails on company-issued smartphone that employee returned upon leaving employer, as would create civil liability under criminal statute prohibiting interception of electronic communications. 18 U.S.C.A. § 2520.

1 Cases that cite this headnote

[13] Torts

Particular cases in general

Former employee's allegations that she returned employer-issued smartphone upon leaving employment, that supervisor accessed her personal e-mail on smartphone over 18 months, and that he shared some of the e-mails were sufficient to state a claim under Ohio law for intrusion into seclusion as an invasion of privacy.

Cases that cite this headnote

[14] Criminal Law

Civil liabilities to persons injured; reparation

Former employee's allegations that she returned employer-issued smartphone upon leaving employment and that supervisor accessed her personal e-mail on smartphone over 18 months were sufficient to state a claim under Ohio statute permitting person injured by another's criminal conduct to recover against perpetrator for supervisor accessing information or telecommunication service without authorization. Ohio R.C. §§ 2307.60, 2913.04(B).

Cases that cite this headnote

[15] Damages

Elements in general

The elements for a claim under Ohio law of intentional infliction of emotional distress (IIED) are: (1) a defendant intended to cause emotional distress, or knew or should have known that his actions would result in serious emotional distress; (2) the defendant's conduct was so extreme and outrageous that it went beyond all possible bounds of decency and can be considered completely intolerable in a civilized community; (3) the defendant's actions proximately caused psychological injury to the plaintiff; and (4) the plaintiff suffered serious mental anguish of a nature no reasonable person could be expected to endure.

Cases that cite this headnote

[16] Damages

Other particular cases

Former employee's allegations that she returned employer-issued smartphone upon leaving employment, that supervisor accessed her personal e-mail on smartphone over 18 months, and that she suffered severe mental anguish were insufficient to state a claim of intentional infliction of emotional distress (IIED) under Ohio law; employee did not allege any psychological injury and allegations as to mental anguish were conclusory.

Cases that cite this headnote

Attorneys and Law Firms

***750** Sarah A. McHugh, Emily C. Zillgitt, Maloney, McHugh & Kolodgy, Toledo, OH, for Plaintiff.

James B. Niehaus, Frantz Ward, Cleveland, OH, for Defendant.

ORDER

JAMES G. CARR, Senior District Judge.

This is a suit by Sandi **Lazette**, a former employee of the defendant Cellco Partnership, ***751** d/b/a Verizon Wireless (Verizon), and her supervisor, defendant **Kulmatycki**. The gravamen of the action is that, after plaintiff left Verizon's employee and returned her company-issued blackberry

(which she used and refers to in her complaint as her "phone"), **Kulmatycki**, during the ensuing eighteen months, read without her knowledge or authorization 48,000 e-mails sent to plaintiff's personal g-mail account. In addition, plaintiff alleges **Kulmatycki** disclosed the contents of some of the e-mails to others.

This alleged conduct gives rise to five claims: 1) violation of the Stored Communications Act (SCA), 18 U.S.C. § 2701 *et seq.*;[1] 2) violation of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III), 18 U.S.C. § 2510 *et seq*;[2] 3) Ohio common law invasion of privacy/seclusion; 4) civil recover for violation of O.R.C. § 2913.04(B);[3] and 5) Ohio common law intentional infliction of emotional distress.

Pending is defendants' motion to dismiss. (Doc. 5). For the reasons that follow, I deny the motion in part and grant it in part.

Background

According to the complaint, the factual allegations of which I take as true, Verizon provided the blackberry for plaintiff's use. She was told that she could use the company-issued phone for personal e-mail. She had an account with g-mail, though she believed she had deleted that account from the phone before giving it to **Kulmatycki** in September, 2010. She understood that Verizon would "recycle" the phone for use by another employee.

In May, 2012, plaintiff learned that **Kulmatycki**, rather than deleting her g-mail account, had been accessing her g-mail account for a period of eighteen months. In addition, **Kulmatycki**, on information and belief, had disclosed the contents of the e-mails he had accessed.

Plaintiff neither consented to nor authorized **Kulmatycki's** surreptitious reading of her personal e-mails. His actions were within the scope and course of his employment with Verizon.

Once plaintiff was aware of **Kulmatycki's** actions, she changed her password to prevent further access. Before she did so, he had accessed 48,000 e-mails in plaintiff's g-mail account. Among the contents of the accessed e-mails were communications about plaintiff's family, career, financials, health, and other personal matters.

Kulmatycki's conduct was knowing, intentional, willful, wanton, malicious, and fraudulent. He undertook his actions to benefit Verizon and further his own interests.[4]

*752 Discussion

1. Stored Communications Act

Section 2701 of the SCA states in pertinent part:

> (a) Offense.—Except as provided in subsection (c) of this section whoever—
>
> > (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> >
> > (2) intentionally exceeds an authorization to access that facility;
>
> and thereby obtains ... access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.
>
> * * * * * *
>
> (c) Exceptions.—Subsection (a) of this section does not apply with respect to conduct authorized—
>
> > (1) by the person or entity providing a wire or electronic communications service; ....[5]

Section 2707 of the SCA provides in pertinent part:

> (a) Cause of action.—... [A]ny ... person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

Relief available under this provision includes equitable relief, damages, and reasonable attorneys' fees and litigation costs. 18 U.S.C. § 2707(b).

The SCA incorporates the definition of "electronic storage" from Title III:

> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

18 U.S.C. § 2510(17).

The defendants assert that **Kulmatycki's** opening and reading 48,000 of plaintiff's e-mails during an eighteen month period did not violate the SCA. In making this argument, they contend:

- The relief plaintiff seeks is not available because the legislative history shows that Congress aimed the SCA at "high-tech" criminals, such as computer hackers;
- **Kulmatycki** had authority to access plaintiff's e-mails;
- **Kulmatycki's** access did not occur *via* "a facility through which an electronic communication service is provided" other than the company owned blackberry;
- The e-mails were not in electronic storage when **Kulmatycki** read them;

***753** • Verizon may be exempt from the SCA under § 2701(c)(1), which states that the person or entity providing an electronic communications service is exempt from the Act, because the complaint does not make clear that plaintiff's g-mail account was separate from her company account. [6]

a. Whether the SCA Applies

[1] Defendants' reading of congressional intent and the case law with regard to whether the SCA prohibits unauthorized access to another person's g-mail account is not persuasive.

In support of their claim that Congress intended the SCA only to reach computer hackers, not someone who reads another person's e-mails without his or her knowledge, defendants cite *Int'l Ass'n of Machinists & Aero. Workers v. Werner–Matsuda*, 390 F.Supp.2d 479, 495 (D.Md.2005).

In that case, the court stated, "Federal courts interpreting these statutes have noted that their 'general purpose ... was to create a cause of action against "computer hackers (*e.g.*, electronic trespassers)." ' " (citing *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F.Supp.2d 817, 820 (E.D.Mich.2000) (quoting *State Wide Photocopy Corp. v. Tokai Fin. Servs., Inc.*, 909 F.Supp. 137, 145 (S.D.N.Y.1995))).

However, the case from which the court in *Machinists* derived its comment about the "general purpose" of the SCA, stated less restrictively: "generally, it appears that the ECPA was *primarily* designed to provide a cause of action against computer hackers, (*i.e.*, electronic trespassers." *State Wide Photocopy, Corp. v. Tokai Financial Services, Inc.* 909 F.Supp. 137, 145 (S.D.N.Y.1995) (emphasis supplied)). "Primarily" does not mean "exclusively," despite defendants' assertion that **Kulmatycki's** conduct is outside the statute's scope because he was not a "hacker" in the conventional sense. [7]

Moreover, the case from which *Machinists* drew its specific language, *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F.Supp.2d 817 (E.D.Mich.2000), also stated expressly, "The provisions of section 2701 of the Act apply to persons or entities in general and prohibit intentional accessing of electronic data without authorization or in excess of authorization." *See also Educational Testing Service v. Stanley H. Kaplan, Educational Center, Ltd.* 965 F.Supp. 731, 740 (D.Md.1997) ("it appears evident that the sort of trespasses to which the Stored Communications Act applies are those in which the trespasser gains access to information to which he is not entitled to see"); *Thayer Corp. v. Reed*, 2011 WL 2682723, *7 (D.Me.) ("The statute does not limit liability to 'hackers.' ").

The prohibitions of the SCA apply to the defendants.

b. Authority to Access Plaintiff's E–Mails

Defendants argue that **Kulmatycki** had authority to access plaintiff's g-mail account because: 1) he used a company-owned blackberry; 2) he did not access a "facility," as the statute uses that term; ***754** and 3) plaintiff authorized **Kulmatycki's** access because she had: a) not expressly told him not to read her e-mails; and b) implicitly consented to his access by not deleting her g-mail account.

i. Use of Company–Owned Device/Authorization

Defendants claim that, because **Kulmatycki** indisputably had authority to use the blackberry on which others were sending e-mails to the plaintiff, he could use it to access those e-mails. In support of this contention, among the cases defendants cite are ones where one family member had accessed e-mails sent to another family member on a family computer. *White v. White,* 344 N.J.Super. 211, 781 A.2d 85, 90–91 (2001); *State v. Poling,* 160 Ohio Misc.2d 84, 938 N.E.2d 1118, 1123 (2010).

Those cases are readily distinguishable, as they involved joint users of a shared computer. Here, there never was joint use between plaintiff and **Kulmatycki**. Indeed, when **Kulmatycki** accessed e-mail sent to plaintiff, she was not able to use the blackberry to do likewise.

Other cases which the defendants cite are similarly inapposite. In *Lasco Foods, Inc. v. Hall and Shaw Sales, Marketing & Consulting, LLC,* 600 F.Supp.2d 1045, 1050 (E.D.Mo.2009), the plaintiff expressly acknowledged the defendants, among whom were former company employees, had "virtually unrestricted access to its information." In other words, at the time the individual defendants had accessed the databases, the plaintiff knowingly, and with its approval, permitted them to do so.

Here, plaintiff neither knew nor approved of **Kulmatycki's** accessing her e-mails. [8]

In *Sherman, supra,* after a former employee sued the defendant for breach of contract, the defendant company sought leave to counter-sue for a violation of the SCA. Its proposed countercomplaint asserted the former employee had used a computer and a company access code, which one of the company's customers had provided, to access sales data on the customer's database. The plaintiff thereafter provided that data to a competitor. 94 F.Supp.2d at 819. [9]

The circumstances in *Sherman* are likewise distinguishable. As in *Lasco,* the party in *Sherman* claiming a violation of § 2701 acknowledged in its complaint that the alleged miscreant had had authority to access the customer's vendor sales database. *Id.* The company's complaint was that its former employee had not had authority to view *its* sales information on that database and thereafter disclose that information. This contention, the court held, did not pass muster under either § 2701, prohibiting unauthorized access, or § 2702, prohibiting disclosure by service providers of the SCA. *Id.* at 820.

***755** What matters here is that the aggrieved party in *Sherman,* unlike plaintiff here, acknowledged that the alleged intruder had had authority to access the database in the first instance.

To be sure, the court in *Sherman* noted that the former employee had not misused the company's password to access the customer's database. *Id.* at 821. Plaintiff's complaint does not allege password misuse as such.

[2] While password misuse did not occur here, it does not matter. I find nothing in the statute or anywhere else that suggests—just as with defendants' claim that only hackers are liable—use of a password somehow is an element which a SCA plaintiff must prove. [10]

[3] I conclude, accordingly, that the mere fact that **Kulmatycki** used a company-owned blackberry to access plaintiff's e-mails does not mean that he acted with authorization when he did so.

ii. Accessing a "Facility"

Section 2701(a)(1) prohibits "intentionally access[ing] without authorization a facility through which an electronic communication service is provided."

Defendants contend that **Kulmatycki's** conduct was lawful, because he used the blackberry to open and read plaintiff's e-mails. Their reasoning is that: 1) the blackberry was a "facility" within the meaning of § 2701(a)(1); 2) **Kulmatycki** was (indisputably) an authorized user of the blackberry; therefore, 3) the SCA permitted him to use such facility to do what he did. Accordingly, defendants conclude, plaintiff fails to state a claim under § 2701.

In support of their argument that the blackberry was a "facility," the defendants point to cases which have held that a personal computer qualifies as a "facility." *See Chance v. Ave. A, Inc.,* 165 F.Supp.2d 1153, 1161 (W.D.Wash.2001); *In re Intuit Privacy Litig.,* 138 F.Supp.2d 1272, 1275 n. 3 (C.D.Cal.2001); *Expert Janitorial, LLC v. Williams,* 2010 WL 908740, *5 (E.D.Tenn.).

I disagree with defendants' reasoning and their contention that a personal computer, much less a blackberry, is a "facility" within § 2701(a)(1).

Neither Title III nor the SCA defines "facility." *Cornerstone Consultants, Inc. v. Production Input Solutions, L.L.C.*, 789 F.Supp.2d 1029, 1050 (N.D.Iowa 2011); *Freedom Banc Mortg. Servs., Inc. v. O'Harra*, 2012 WL 3862209, *9 (S.D.Ohio).

The recent decision in *In re iPhone Application Litigation*, 844 F.Supp.2d 1040 (N.D.Cal.2012), makes clear that a cell phone is not a "facility." After emphasizing, "the computer systems of an email provider, a bulletin board system, or an ISP are uncontroversial examples of facilities that provide electronic communications services to multiple users," the court also acknowledged, "less consensus surrounds the question presented here: whether an individual's computer, laptop, or mobile device fits the statutory definition of a 'facility through which an electronic communication service is provided.' " *Id.* at 1058.

The court in *iPhone* then turned its attention to the cases, noted above, which ***756** have equated a personal computer to be a § 2701(a)(1) "facility." Those cases, in the court's view, "provide little analysis on this point of law, instead assuming plaintiff's position to be true due to lack of argument and then ultimately ruling on other grounds." *Id.* at 1058–59.

Finding these cases, as I do, unhelpful, the court in *iPhone* looked to and followed the decision in *Crowley v. CyberSource Corp.*, 166 F.Supp.2d 1263, 1271 (N.D.Cal.2001). In *Crowley* the court pointed out that, if the computer which is accessed and the computer through which access occurs are both "facilities," it would certainly "seem odd that the provider of a communication service could grant access to one's home computer to third parties, but that would be the result of Crowley's argument." Taking this circuitous route, the court observed, "would equate a user with a provider and, thus, ignore language in § 2701(c) that treats users and providers as different." *Id.* at 1270. A user of a service, as **Kulmatycki** was when he accessed plaintiff's e-mails, is not also the provider of those same e-mails.

[4] Thus, the better, more sensible, and harmonious reading of the SCA is that a personal computer, and, *ergo*, a blackberry or cell phone, is not a "facility" within § 2701(a)(1).

Several other courts agree that devices with which a user accesses electronic communications are not "facilities." *Garcia v. City of Laredo*, 702 F.3d 788, 792–93 (5th Cir.2012); *Cornerstone Consultants, supra*, 789 F.Supp.2d at 1050 (pertinent "facility" through which an electronic communication service is provided is e-mail server); *Freedom Banc, supra*, 2012 WL 3862209, *8 ("the relevant 'facilities' that the SCA is designed to protect are not computers that enable the use of an electronic communication service, but instead are facilities that are operated by electronic communication service providers and used to store and maintain electronic storage.").

Instead, the "electronic communications service" resided in the g-mail server, not on the blackberry, and the g-mail server, not the blackberry, was the "facility."

iii. Plaintiff did not Authorize Access to her E–Mails

Plaintiff deleted the e-mails she had received before leaving Verizon. But she did not also close her g-mail account, though she believed she had done so. Her failure to be more careful, defendants contend, deprives her of any claim under the SCA.

Defendants correctly contend that the essence of plaintiff's complaint is that **Kulmatycki** accessed her e-mails without her consent. According to them, the plaintiff negligently and/or implicitly consented to his doing so when she returned the blackberry without having ensured that she had deleted her g-mail account.

[5] Defendants also point out that plaintiff's complaint does not allege that **Kulmatycki** took any affirmative steps to cause the device to receive e-mails. Nothing in the SCA requires one who accesses a service provider without authorization also to have done something to the equipment to facilitate his access.[11] To the extent ***757** that plaintiff has to prove the **Kulmatycki** did anything "affirmative," she has done so *via* her contention that he read her e-mails. Doing so required opening the e-mails, which was an affirmative act on his part.

[6] Turning to the substance of defendants' contentions, defendants, in effect, contend that plaintiff's negligence left her e-mail door open for **Kulmatycki** to enter and roam around in for as long and as much as he desired.

[7] This is an unacceptable reading of § 2701(a)(1), which prohibits "access without authorization," and of the private party consent surveillance provision, 18 U.S.C. § 2511(2)(d). [12] To be sure, consent under this provision need not be explicit, it can, as defendants allege, also be implied. *Williams v. Poulos,* 11 F.3d 271, 281 (1st Cir.1993). Negligence is, however, not the same as approval, much less authorization. There is a difference between someone who fails to leave the door locked when going out and one who leaves it open knowing someone be stopping by.

Whether viewed through the lens of negligence or even of implied consent, there is no merit to defendants' attempt to shift the focus from **Kulmatycki's** actions to plaintiff's passive and ignorant failure to make certain that the blackberry could not access her future e-mail. On this issue, a case involving a claim of implied consent under 18 U.S.C. § 2511(2)(d), *Griggs–Ryan v. Smith,* 904 F.2d 112 (1st Cir.1990), is instructive:

> [I]mplied [consent] is "consent in fact" which is inferred "from surrounding circumstances indicating that the [party] *knowingly agreed to the surveillance.*" Thus, implied consent—or the absence of it—may be deduced from "the circumstances prevailing" in a given situation. The circumstances relevant to an implication of consent will vary from case to case, but the compendium will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private. And the ultimate determination must proceed in light of the prophylactic purpose of Title III—a purpose which suggests that consent should not casually be inferred.

Id. at 116–17. (citations omitted) (emphasis supplied). *Accord, Williams, supra,* 11 F.3d at 281.

Indeed, even "knowledge of the capability of monitoring alone cannot be considered implied consent." *Deal v. Spears,* 980 F.2d 1153, 1157 (8th Cir.1992). In that case the court held an employee did not impliedly consent to monitoring of her phone calls when her employer only told her that it might monitor phone calls. *Id.* In this case, where plaintiff believed she had eliminated her g-mail account from the blackberry, she was unaware of the possibility that others might access her future e-mails from that account.

What it takes to find implied consent shows clearly that plaintiff here did give such consent. Thus, in *U.S. v. Workman,* 80 F.3d 688, 693 (2d Cir.1996), the court found an inmate had impliedly consented where a notice by the telephone and prison handbook told him calls would be monitored. Similarly, in *Griggs–Ryan, supra,* 904 F.2d at 118, the plaintiff had been told several times that monitoring of phone calls would occur. In *Shefts v. Petrakis,* 758 F.Supp.2d 620, 631 (C.D.Ill.2010), the court found implied consent where the employee ***758** manual informed him text messages would be logged.

[8] Consent to access otherwise private electronic communications can, under § 2511(2)(d), constitute authorization to read those communications. Even when a party gives such consent, it is limited by its own terms. An inmate who knows his phone conversations with a friend might be monitored does not expose his communications with his attorney to a jailer's ear. Here, even if plaintiff were aware that her e-mails might be monitored, any such implied consent that the law might perceive in that knowledge would not be unlimited. Random monitoring is one thing; reading everything is another.

c. Electronic Storage

The defendants claim that the complaint fails to allege sufficient facts to establish that the e-mails **Kulmatycki** accessed were in "electronic storage" when he accessed them. As previously noted, the SCA incorporates the definition of "electronic storage" in § 2510(17) of Title III: "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for the purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

The defendants argue, and several courts have agreed, that only e-mails awaiting opening by the intended recipient are within this definition. *In re DoubleClick, Inc. Privacy Litig.,* 154 F.Supp.2d 497, 511–12 (S.D.N.Y.2001); *Fraser v. Nationwide Mut. Ins. Co.,* 135 F.Supp.2d 623, 635–36 (E.D.Pa.2001); *U.S. v. Weaver,* 636 F.Supp.2d 769, 771 (C.D.Ill.2009); *Hilderman v. Enea TekSci, Inc.* 551 F.Supp.2d 1183, 1205 (S.D.Cal.2008) ("courts have construed subsection (A) as applying to e-mail messages stored on an ISP's server pending delivery to the recipient, but not e-mail messages remaining on an ISP's server after delivery."); *Jennings v. Jennings,* 401 S.C. 1, 736 S.E.2d 242, 245 (2012). [13] E-mails which an intended recipient

has opened may, when not deleted, be "stored," in common parlance. But in light of the restriction of "storage" in § 2510(17)(B) solely for "backup protection," e-mails which the intended recipient has opened, but not deleted (and thus which remain available for later re-opening) are not being kept "for the purposes of backup protection." *Jennings, supra,* 736 S.E.2d at 245.

[9] Thus, plaintiff cannot prevail to the extent that she seeks to recover based on a claim that **Kulmatycki** violated the SCA when he accessed e-mails which she had opened but not deleted. Such e-mails were not in "backup" status as § 2510(17)(B) uses that term or "electronic storage" as § 2701(a) uses that term.

[10] With regard to e-mails which plaintiff had yet to open before **Kulmatycki** did so, defendants argue that her allegations about her unopened e-mails being in electronic storage fail the *Twombly/Iqbal* test. This is so, because plaintiff does not specify which of the 48,000 e-mails which ***759** **Kulmatycki** allegedly accessed were awaiting opening by plaintiff.

Given the volume of e-mails which plaintiff alleges **Kulmatycki** opened, I believe that I can draw a fair and plausible inference that **Kulmatycki** opened some of those e-mails before plaintiff did, and thus, in doing so, violated § 2701(a). [14]

Plaintiff's complaint adequately alleges that **Kulmatycki** violated § 2701(a) when he opened e-mails before she did.

In light of the foregoing, I overrule defendants' complaint to the extent that it seeks dismissal *in toto* of plaintiff's SCA claim. I grant it, however, to the extent that plaintiff seeks to recover for his opening of e-mails which she had opened before he did.

d. Verizon's Vicarious Liability

[11] Plaintiff alleges, and defendants acknowledge, that **Kulmatycki's** actions were within the scope of his employment by Verizon and in furtherance of its interest. Defendants seek dismissal of Verizon on the basis that it may be exempt from liability under § 2701(c)(1). That provision states that an entity providing an electronic communications service is exempt from the Act.

In support of this supposition, defendants contend that the complaint does not make clear whether plaintiff's g-mail account was separate from the account Verizon provided for her work-related use. If so, then, according to defendants, Verizon would have become a provider of electronic communication services and within the exemption of § 2701(c)(1).

Once again, defendants look outside the four corners of plaintiff's complaint for assistance. All that plaintiff had to assert was that she had a g-mail account and **Kulmatycki** accessed her emails without authorization. She has done so.

It is up to defendants to develop the evidentiary and legal basis for their challenge, which is in the nature of an affirmative defense. A plaintiff does not bear the burden of anticipating defenses and pleading over them in order to avoid Rule 12(b) dismissal. *Veney v. Hogan,* 70 F.3d 917, 921 (6th Cir.1995) ("the plaintiff need not fully anticipate the defense in the complaint"), *overruled in part on other grounds, Goad v. Mitchell,* 297 F.3d 497 (6th Cir.2002).

Plaintiff has, in any event, asserted, and defendants have admitted that **Kulmatycki** was acting within the scope of his employment and in furtherance of Verizon's interests when he accessed plaintiff's e-mails. Defendants' motion does not challenge plaintiff's actual theory of liability—namely, that Verizon is vicariously liable for **Kulmatycki's** actions, much less shown that conventional master-servant liability law does not apply.

***760** I overrule defendants' motion to dismiss Verizon.

2. Title III

[12] Plaintiff claims that **Kulmatycki's** conduct included not only accessing her stored electronic communications, but disclosing those communications to others. This, she contends, gives rise to a cause of action under 18 U.S.C. § 2520, the civil liability provision of Title III.

Defendants claim that plaintiff has failed to state a cause of action under § 2520. They base their contention on two provisions of Title III, 18 U.S.C. § 2510(4) and § 2510(5), found in the statute's definition section.

Section 2510(4) defines "intercept" to mean "the aural or other acquisition of the contents of any wire, electronic,

or oral communication through the use of any electronic, mechanical, or other device."

Section 2510(5) defines "electronic, mechanical, or other device" to mean "any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than" certain exceptions not applicable here.

The term "interception" in § 2510(4) does not encompass electronic communications stored, as the e-mails here were, for the intended recipient's retrieval on her own computer. *E.g.*, *Fraser v. Nationwide Mutual Insurance Co.*, 352 F.3d 107, 113 (3d Cir.2003); *Steve Jackson Games, Inc. v. Secret Service*, 36 F.3d 457 (5th Cir.1994); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir.2002); *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir.2003).

In response, plaintiff points to the Seventh Circuit's decision in *U.S. v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir.2010). In that case, the defendant installed a "rule" on his supervisor's computer. The device caused the defendant's computer to receive the e-mail whenever the supervisor's e-mail service provider sent a message to the supervisor's computer. *Id.* at 703. Thus, the defendant acquired the e-mail from the service provider directly and concurrently, not by later accessing the service provider's computer. Receipt of the e-mail by each within "no more than an eyeblink" constituted interception by the defendant under § 2510(5). *Id.* at 706.

Here, in contrast, **Kulmatycki** went to the server's computer, where plaintiff's g-mail account was to be found. By then, g-mail had already sent the message to plaintiff's computer.

Kulmatycki did not, therefore, "intercept" plaintiff's e-mail, and Title III does not cover his actions.

That being so, the defendants' motion to dismiss plaintiff's Title III claim is well-taken. [15]

3. Invasion of Privacy: Intrusion into Seclusion

Plaintiff claims that **Kulmatycki's** actions give rise to an Ohio common-law tort claim for invasion of privacy/ intrusion into seclusion. With regard to such claim, the court in *Moore v. Univ. Hospitals of Cleveland Medical Center*, 2011 WL 5554272, *4 (N.D.Ohio) stated:

> Citing Section 652B of the Restatement of Torts 2d, the Ohio Supreme Court [has] said, "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." *Sustin v. Fee*, 69 Ohio St.2d 143, 431 N.E.2d 992, 993–94 (Ohio 1982). The key language is that the affairs or concerns ***761** must be private to rise to be actionable as an invasion of privacy. *See Olson v. Holland Computers, Inc.*, 2007 WL 2694202, at *4 (Ohio Ct.App.2007) ("In order to establish a wrongful intrusion into private activities, a plaintiff must show that he or she had a reasonable expectation of privacy in the area allegedly intruded.")

In *Moore*, the court granted summary judgment to the defendant as to plaintiff's claim that it had "broken into" the e-mail account which the defendant provided. The court found the plaintiff had failed to allege evidence to support his claim. In addition, it also found plaintiff had not established, in the face of defense evidence of warnings about monitoring, that he had had a reasonable expectation of privacy. *Id.*, *4.

Although this decision properly states the applicable law as to the elements of plaintiff's claim, defendants' reliance on it to justify dismissal is misplaced. This is so, because, as plaintiff points out, I cannot consider the contents of defendants' employee handbook, which it attached an exhibit to the motion to dismiss. Considering that exhibit, much less whether it constituted a defense to plaintiff's claim would, at this stage, be entirely premature.

Moreover, it would be one-sided. Courts in Ohio apply a totality of the circumstances test to determine whether an individual has a reasonable expectation of privacy. *See, e.g.*, *State v. Corbin*, 194 Ohio App.3d 720, 727, 957 N.E.2d 849 (2011); *see also Savoy v. U.S.*, 604 F.3d 929, 935 (6th Cir.2010) (applying state totality of circumstances law in case involving state tort claims of intrusion *via* videotaping).

[13] Many factors can affect whether plaintiff's expectations that no one would intrude into her e-mail account, particularly in light of her unawareness of **Kulmatycki's** ability to do so. Indeed, the precise terms of the warning matter. With regard to what one might expect from a warning of the possibility of occasional, random monitoring is one thing, total absorption is another. Here there are, in any event, several preliminary issues that have yet to be addressed. Among these, aside from

the content of the warning, are just what did **Kulmatycki** do, when did he do it, what were his motives, when might plaintiff have become aware of his intrusions, and what and from whom had she learned about using her company blackberry for a personal e-mail account. These and other factors may have a bearing on the reasonableness of what plaintiff might reasonably have expected when she returned her blackberry.

Otherwise, with regard to the elements of this tort, I find plaintiff's claim survives the pending motion. Her e-mails were highly personal and private. A reasonable jury could find **Kulmatycki's** reading of tens of thousands of such private communications, if proven to have occurred, "highly offensive."

I find that plaintiff has stated a viable claim for privacy/intrusion into seclusion. *See Eysoldt v. ProScan Imaging*, 194 Ohio App.3d 630, 639, 957 N.E.2d 780 (Ohio App.2011) (evidence sufficient that defendant turned plaintiff's e-mail accounts over to third party who could read them).

4. Claim Under O.R.C. § 2913.04

[14] Plaintiff asserts a claim under O.R.C. §§ 2307.60, .61, which permit a person injured by another's criminal conduct to recover against the perpetrator of the crime. In this case, O.R.C. § 2913.04(B) defines the crime on which plaintiff bases her claim:

> No person, in any manner and by any means, including, but not limited to, computer hacking, shall knowingly gain access to, attempt to gain access to, or ***762** cause access to be gained to any computer, computer system, computer network, cable service, cable system, telecommunications device, telecommunications service, or information service without the consent of, or beyond the scope of express or implied consent of, the owner of the computer, computer system, computer network, cable service, cable system, telecommunications device, telecommunications service, or information service or other person authorized to give consent.

The defendants assert two ground for dismissal: plaintiff did not own the blackberry, so that they were entitled to use it to gain access to her g-mail account, and, in any event, the statutory purpose is to deter computer hacking.

Defendants misread these very broad and inclusive provisions of this remedial statute. It says nothing about who owns the means of intrusion: indeed, it is as likely that an intruder would use his or her own device as he or she would use someone else's device to gain access to that person's computer or computer-based information.

Second, and even more completely off the mark, the defendants claim that this is simply an anti-hacking statute, and has nothing to do with a finding out something that he or she has no business or right to find out. By its own terms, the statute states, "including but not limited to, computer hacking." In plain English, "including but not limited to" is not a term of limitation, but one of limitless expansion.

In any event, cases applying O.R.C. § 2913.04(B) have encompassed a broad range of misconduct. Appellate courts have upheld convictions of defendants who have: misused a work computer to access a work-related database with a personal, non-work related motive, *State v. Claborn*, 2012 WL 1078930, *2 (Ohio App.), entered computer network and caused damage, *State v. Holt*, 2011 WL 1204330, *1 (Ohio App.), locked the victims out of their internet accounts, used the victims' names to send vulgar messages to others, and sent vulgar messages about the victims to others, *State v. Cline*, 2008 WL 1759091, *1 (Ohio App.), continued using a cable box after disconnection without provider's consent, *State v. Sullivan*, 2003 WL 22510808, *4 (Ohio App.), improperly accessed law enforcement criminal records database, *State v. Moning*, 2002 WL 31127751, *1 (Ohio App.), used another's phone to make long distance calls, *State v. McNichols*, 139 Ohio App.3d 252, 254, 743 N.E.2d 500 (Ohio App.2000), improperly accessed Law Enforcement Automated Data system, *State v. Giannini*, 1998 WL 886961, *1 (Ohio App.), committed telephone toll fraud, *State v. Redd*, 1994 WL 178451, *1 (Ohio App.), and installed password protected software on workplace computer without authorization. *State v. Johnson*, 1992 WL 25312, *1 (Ohio App.).

The plaintiff has stated a claim under O.R.C. §§ 2307.60, .61 and § 2913.04(B).

5. Intentional Infliction of Emotional Distress

Plaintiff's final claim is for intentional infliction of emotional distress.

[15] The elements of such claim are:

> (1) the defendant intended to cause emotional distress, or knew or should have known that his actions would result in serious emotional distress; (2) the defendant's conduct was so extreme and outrageous that it went beyond all possible bounds of decency and can be considered completely intolerable in a civilized community; (3) the defendant's actions proximately caused psychological injury to the plaintiff; and (4) the plaintiff suffered serious mental anguish of a nature no reasonable person could be expected to endure.

***763** *Yeager v. Local Union 20,* 6 Ohio St.3d 369, 453 N.E.2d 666 (1983) *Yeager v. Local Union 20* (1983) (syllabus).

The defendants argue that plaintiff's allegations relating to mental anguish are insufficient. Even aside from *Twombly/Iqbal,* the pleading requirement with regard to the injury are quite high: namely, that the defendant's actions "caused psychological injury," and "plaintiff suffered serious mental anguish."

[16] Plaintiff's complaint makes no allegation of psychological injury. More importantly, her claim of having suffered severe mental anguish is entirely conclusory. That being so, I conclude that it is insufficient under the *Twombly/Iqbal* standard. *See Foxx v. Healix Infusion Therapy, Inc.*, 2013 WL 791188, *7 (E.D.Tenn.) ("plaintiff does not sufficiently allege a serious mental injury as required for the claim. Plaintiff merely alleges in conclusory fashion that her termination 'would cause the Plaintiff severe emotional distress' and that she suffered 'humiliation and embarrassment, and emotional distress.' ").

I shall, however, grant plaintiff four weeks from the date of entry of this order to file an amended complaint in which she states that she either has been undergoing treatment for psychic injuries, suffered specific and prolonged psychic and/or psychic-related consequences, or both. *See, e.g., Buckman–Peirson v. Brannon,* 159 Ohio App.3d 12, 21, 822 N.E.2d 830 (2004). If plaintiff fails to file an amended complaint stating a plausible claim for intentional infliction of emotional injuries, this count shall be dismissed with prejudice.

Conclusion

For the foregoing reasons, it is

ORDERED THAT:

1. Defendants' motion to dismiss plaintiff's claims under 18 U.S.C. § 2520 and claims under 18 U.S.C. § 2701 to the extent she seeks § 2701 recovery for accessing opened, but undeleted e-mail, be, and the same hereby is granted;

2. Defendants' motion to dismiss plaintiff's other claim for violation of the Stored Communications Act and her state law claims for civil recovery for criminal acts, and invasion of privacy-seclusion be, and the same hereby is overruled;

3. Defendants' motion to dismiss plaintiff's claim for intentional infliction of emotional distress be, and the same hereby is denied, subject to plaintiff's filing within four weeks of the date of this order of an amended complaint as required herein; if plaintiff fails to files an amended complaint within that time, defendants' motion to dismiss this count shall be granted.

The Clerk shall forthwith set a status/scheduling conference.

So ordered.

Footnotes

1 18 U.S.C. § 2707 provides a cause of action for violations of the SCA

2 18 U.S.C. § 2520 provides a cause of action for violations of Title III.

3 O.R.C. §§ 2307.60, 2307.61 provide a cause of action for persons injured by another's felonious conduct.

4 The defendants' motion to dismiss contains numerous factual allegations that more properly belong, if evidentiary support exists for them, and if there is no dispute about them, in a motion for summary judgment. I have ignored those allegations.

The motion to dismiss also suggests that the complaint generally fails to meet the *Twombly/Iqbal* pleading requirements. *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007). With one exception (relating to her intentional infliction of emotional distress claim), I disagree: plaintiff's complaint amply sets forth "enough facts to state [claims] to relief that [are] plausible on [their] face." *Twombly*, 550 U.S. at 570, 127 S.Ct. 1955. Most simply, those well-plead facts allege **Kulmatycki**, without authorization, over an eighteen month period, accessed 48,000 e-mails in plaintiff's personal g-mail account. The fact that the complaint also—and properly so—recites or paraphrases statutory language does not somehow negate the plausibility of the claim she asserts under the statute, or take her complaint into *Twombly/Iqbal* territory. *Cf. Monson v. Whitby School, Inc.*, 2010 WL 3023873, *3 (D.Conn.) ("while Dr. Monson argues that Whitby's [SCA] allegation that her actions were 'unauthorized' is too 'conclusory' to state a viable claim, it is difficult to imagine how else Whitby could plead this necessary element." other than to assert actions were beyond scope of any authority).

5 Sections 2703 (required disclosure of customer records), 2704 (backup storage), and 2518 (court orders for law enforcement electronic surveillance) are not applicable to what is presently at issue in this case.

6 I disagree with this contention. The complaint alleges the blackberry "contained both professional and personal email accounts." (Doc. 1, ¶ 3). It is clear from the complaint that plaintiff is talking about an account separate and distinct from her company-provided e-mail account.

7 The statement in *Wide Photo.* was, moreover, dictum, as on the dissimilar facts of that case, the court did not depend on the statute's putative purposes—primary or otherwise—in dismissing the complaint. 909 F.Supp. at 146 ("State Wide's § 2702 claim is deficient in the same fashion as the § 2701 claim in failing to allege facts demonstrating that Tokai is covered by the described categories of prohibited actors or that State Wide is an aggrieved party within the meaning of the ECPA.").

8 In *Lasco,* the plaintiff alleged the defendants had exceeded the scope of their authority when accessing company databases before leaving the plaintiff's employ. Rejecting this contention, the court noted the lack of factual support for that allegation in the complaint, and pointed out the plaintiff "has not identified any restricted information that Defendants supposedly accessed." 600 F.Supp.2d at 1050.

In this case, because I find that **Kulmatycki** lacked authority to access plaintiff's e-mails, at least to the extent that she had yet to open them, I need not reach the issue of whether **Kulmatycki** violated § 2701(a)(2), which makes liable one who "intentionally exceeds an authorization to access that facility". If, however, I were to find that somehow **Kulmatycki** had a right of access, he exceeded it by exercising that putative authority 48,000 times over an eighteen month period.

9 When the former employee had left the plaintiff's employ, it had instructed to customer to deny access to the customer's database. When the events giving rise to the complaint in *Sherman* occurred, the customer had not followed that instruction. 94 F.Supp.2d at 819.

10 If **Kulmatycki** had authorization to access plaintiff's g-mail account, he necessarily would have had authorization to use her password. If allowed to enter, he was entitled to use the key. This circumstance distinguishes cases finding password misuse. *State Analysis, Inc. v. American Financial Services Assoc.*, 621 F.Supp.2d 309, 318 (E.D.Va.2009); *Cardinal Health 414, Inc. v. Adams*, 582 F.Supp.2d 967, 977 (M.D.Tenn.2008) (former employee who used former co-worker's log-in information "plainly violated the SCA as a matter of law.").

11 I also reject any suggestion that plaintiff has to prove that she affirmatively instructed **Kulmatycki** and Verizon that they were not permitted to access her g-mail account. To be sure, the court in *Sherman, supra,* found no SCA violation because, as to the former employee, there was never a "clear[ ] and [ ] explicit restriction on access." 94 F.Supp.2d at 821. I find nothing in the statute that requires this sort of prophylaxis as a prerequisite to imposing liability on an unknown and unexpected electronic intruder. At most, if at all, the absence of such directive might be a consideration when determining damages from the intrusion.

12 Section 2518(2)(d) provides, "[i]t shall not be unlawful under this chapter for a person ... to intercept a[n] ... electronic communication ... where one of the parties to the communication has given prior consent to such interception."

13 Courts taking a contrary view, and concluding that § 2510(17)(B) "backup storage" includes opened, undeleted e-mails are in a minority and involve, in my view, a strained reading of that provision. *See Theofel v. Farey–Jones*, 359 F.3d 1066, 1071 (9th Cir.2004) ("prior access is irrelevant to whether the [e-mails] at issue were in electronic storage."). *See generally* Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L.Rev. 1208, 1217 (2004) ("*Theofel* is quite implausible and hard to square with the statutory test."). Moreover, that the Sixth Circuit would follow *Theofel* and extend SCA protection to opened but undeleted e-mails is doubtful. *See U.S. v. Warshak*, 631 F.3d 266, 291 (6th Cir.2010) (quoting Kerr, *supra*).

14 At this stage of this case, it appears that the extent of **Kulmatycki's** violation is a matter of damages, rather than of liability *ab initio.* While the jury cannot speculate as to damages, it can consider circumstantial proof as to such issues as how often and when plaintiff and **Kulmatycki** accessed her g-mail account. Or, it may be possible (though I simply don't know whether it is), for forensic analysis

to ascertain when each of them accessed a message, and thereby, possibly, arrive at a very precise figure with regard to which e-mails plaintiff had and had not opened before **Kulmatycki** did.

These are matters for the forthcoming stages of this case. For now, I only conclude that plaintiff has stated a plausible, albeit circumstantial, claim that **Kulmatycki** opened some e-mails before she did. After all, 48,000 e-mails during an eighteen-month period is a daily average of something less than 100. That **Kulmatycki** opened some of plaintiff's e-mails before she did is likely enough for now. On the other hand, it is highly unlikely that he opened, on average, 100 of plaintiff's e-mails every day before she did.

15 It is not necessary to consider the parties' arguments about **Kulmatycki's** use of a “device” under the statute, as that is a moot issue in light of the lack of interception in this case.

End of Document

Supreme Court of New Jersey.
Marina STENGART, Plaintiff–Respondent,
v.
LOVING CARE AGENCY, INC., Steve Vella, Robert Creamer, Lorena Lockey, Robert Fusco, and LCA Holdings, Inc., Defendants–Appellants.

Argued Dec. 2, 2009.
Decided March 30, 2010.

Background: Former nongovernment employee filed action against employer for alleged violations of Law Against Discrimination. Employee applied for order to show cause seeking to require employer to return all copies of e-mail messages exchanged between employee and her attorneys over work-issued laptop computer through employee's personal, password-protected, web-based e-mail account. The Superior Court, Law Division, Bergen County, Estela M. De La Cruz, J.S.C., 2009 WL 798044, converted the application to a motion and denied the motion. Employee's motion for leave to appeal was granted. The Superior Court, Appellate Division, 408 N.J.Super. 54, 973 A.2d 390, reversed and remanded. Employer's motion for leave to appeal was granted.

Holdings: The Supreme Court, Rabner, C.J., held that:
(1) employee had objectively reasonable expectation of privacy in pre-suit e-mail messages exchanged between employee and her attorneys;
(2) e-mail messages were protected by attorney-client privilege;
(3) employer's counsel violated professional conduct rule regarding handling of communications inadvertently sent to a lawyer; and
(4) remand was necessary, for hearing on what sanctions, if any, should be imposed on employer's counsel.

Judgment of Appellate Division affirmed as modified; remanded.

West Headnotes

[1] Privileged Communications and Confidentiality 311H 106

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk106 k. Purpose of privilege. Most Cited Cases

The primary rationale for the attorney-client privilege is to encourage free and full disclosure of information from the client to the attorney, and that, in turn, benefits the public, which is well served by sound legal counsel based on full, candid, and confidential exchanges. N.J.S.A. 2A:84A–20; N.J.S.A. 2A:84A, App. A, Rules of Evid., N.J.R.E. 504.

[2] Privileged Communications and Confidentiality 311H 141

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk135 Mode or Form of Communications
311Hk141 k. E-mail and electronic communication. Most Cited Cases

E-mail exchanges are covered by the attorney-client privilege like any other form of communication. N.J.S.A. 2A:84A–20; N.J.S.A. 2A:84A, App. A, Rules of Evid., N.J.R.E. 504.

[3] Privileged Communications and Confidential-

ity 311H 141

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk135 Mode or Form of Communications
311Hk141 k. E-mail and electronic communication. Most Cited Cases

Privileged Communications and Confidentiality 311H 156

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk156 k. Confidential character of communications or advice. Most Cited Cases

The reasonable-expectation-of-privacy standard derived from the Search and Seizure Clauses of both the Fourth Amendment and the New Jersey Constitution did not apply when determining whether former nongovernment employee had a reasonable expectation of privacy in e-mail messages exchanged between employee and her attorneys over work-issued laptop computer through employee's personal, password-protected, web-based e-mail account, so that the e-mails, which were exchanged before employee filed employment discrimination suit against employer, were protected by attorney-client privilege; rather, a common law reasonable-expectation-of-privacy standard derived from the tort of intrusion on seclusion was applicable. U.S.C.A. Const.Amend. 14; N.J.S.A. Const. Art. 1, par. 7; N.J.S.A. 2A:84A–20; N.J.S.A. 2A:84A, App. A, Rules of Evid., N.J.R.E. 504.

[4] Torts 379 340

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)2 Intrusion
379k340 k. In general. Most Cited Cases

Under the common law tort of intrusion on seclusion, one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person. Restatement (Second) of Torts § 652B.

[5] Torts 379 340

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)2 Intrusion
379k340 k. In general. Most Cited Cases

A high threshold must be cleared to assert a cause of action based on the common law tort of intrusion on seclusion, i.e., a plaintiff must establish that the intrusion would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object. Restatement (Second) of Torts § 652B comment.

[6] Torts 379 340

379 Torts
379IV Privacy and Publicity
379IV(B) Privacy
379IV(B)2 Intrusion
379k340 k. In general. Most Cited Cases

The reasonableness of a claim for the common law tort of intrusion on seclusion has both a subjective and objective component.

[7] Labor and Employment 231H 87

231H Labor and Employment
231HIII Rights and Duties of Employers and

Employees in General
231Hk87 k. Privacy in general. Most Cited Cases

Whether an employee has a reasonable expectation of privacy in her particular work setting must be addressed on a case-by-case basis.

[8] Labor and Employment 231H 96

231H Labor and Employment
231HIII Rights and Duties of Employers and Employees in General
231Hk92 Searches
231Hk96 k. Computers; electronic data storage. Most Cited Cases

Former nongovernment employee had subjective expectation of privacy in e-mail messages exchanged between employee and her attorneys over work-issued laptop computer through employee's personal, password-protected, web-based e-mail account before employee filed employment discrimination suit against employer; employee plainly took steps to protect the privacy of those e-mails and shield them from her employer by not using an employer-based e-mail account and by not saving her personal e-mail account's password on her laptop. N.J.S.A. 2A:84A–20; N.J.S.A. 2A:84A, App. A, Rules of Evid., N.J.R.E. 504.

[9] Labor and Employment 231H 96

231H Labor and Employment
231HIII Rights and Duties of Employers and Employees in General
231Hk92 Searches
231Hk96 k. Computers; electronic data storage. Most Cited Cases

Former nongovernment employee had objectively reasonable expectation of privacy in e-mail messages exchanged between employee and her attorneys over work-issued laptop computer through employee's personal, password-protected, web-based e-mail account before employee filed employment discrimination suit against employer; employer's written policy on electronic communications did not address the use of personal, web-based e-mail accounts accessed through company equipment nor did it warn employees that contents of e-mails sent via personal accounts could be forensically retrieved and read by employer, and the e-mails were not illegal or inappropriate material stored on employer's equipment, which might harm employer in some way, and instead were conversations between a lawyer and client about confidential legal matters, which were historically cloaked in privacy.

[10] Privileged Communications and Confidentiality 311H 141

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk135 Mode or Form of Communications
311Hk141 k. E-mail and electronic communication. Most Cited Cases

Privileged Communications and Confidentiality 311H 156

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk156 k. Confidential character of communications or advice. Most Cited Cases

Former employee had objectively reasonable intent that her communications with her attorneys would be made in confidence, as required for attorney-client privilege, as to e-mail messages exchanged between employee and her attorneys over work-issued laptop computer through employee's personal, password-protected, web-based e-mail account before employee filed employment discrimination suit

against employer; employee plainly took steps to protect the privacy of those e-mails and shield them from her employer by not using an employer-based e-mail account and by not saving her personal e-mail account's password on her laptop, and employer's written policy on electronic communications did not address the use of personal, web-based e-mail accounts accessed through company equipment nor did it warn employees that contents of e-mails sent via personal accounts could be forensically retrieved and read by employer. N.J.S.A. 2A:84A–20; N.J.S.A. 2A:84A, App. A, Rules of Evid., N.J.R.E. 504.

[11] Privileged Communications and Confidentiality 311H 168

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk168 k. Waiver of privilege. Most Cited Cases

Former employee did not fail to take reasonable steps to insure and maintain the confidentiality of e-mail messages, as would waive attorney-client privilege with respect to e-mail messages exchanged between employee and her attorneys over work-issued laptop computer through employee's personal, password-protected, web-based e-mail account before employee filed employment discrimination suit against employer; employee chose not to use an employer-based e-mail account and not to save her personal e-mail account's password on her laptop. N.J.S.A. 2A:84A–20, 2A:84A–29; N.J.S.A. 2A:84A, App. A, Rules of Evid., N.J.R.E. 504, 530.

[12] Privileged Communications and Confidentiality 311H 168

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk168 k. Waiver of privilege. Most Cited Cases

Former employee did not knowingly disclose the information contained in e-mail messages, as would waive attorney-client privilege with respect to e-mails exchanged between employee and her attorneys over work-issued laptop computer through employee's personal, password-protected, web-based e-mail account before employee filed employment discrimination suit against employer; employee was unsophisticated in the use of computers and did not know that employer could read communications sent on her personal e-mail account. N.J.S.A. 2A:84A–20, 2A:84A–29; N.J.S.A. 2A:84A, App. A, Rules of Evid., N.J.R.E. 504, 530.

[13] Labor and Employment 231H 50

231H Labor and Employment
231HI In General
231Hk49 Manuals, Handbooks, and Policy Statements
231Hk50 k. In general. Most Cited Cases

Labor and Employment 231H 766

231H Labor and Employment
231HVIII Adverse Employment Action
231HVIII(A) In General
231Hk760 Reasons or Grounds for Adverse Action
231Hk766 k. Disobedience or insubordination. Most Cited Cases

Employers can adopt lawful policies relating to employees' computer use, to protect the assets, reputation, and productivity of a business and to ensure compliance with legitimate corporate policies, and employers can enforce such policies by disciplining employees and, when appropriate, terminating them, for violating proper workplace rules that are not inconsistent with a clear mandate of public policy.

[14] Labor and Employment 231H 50

231H Labor and Employment
231HI In General
231Hk49 Manuals, Handbooks, and Policy Statements
231Hk50 k. In general. Most Cited Cases

An employer's computer use policy banning all personal use of company computers by employees and providing unambiguous notice that the employer could retrieve and read an employee's attorney-client communications, if accessed on a personal, password-protected e-mail account using the company's computer system, would violate public policy and would not be enforceable. N.J.S.A. 2A:84A–20; N.J.S.A. 2A:84A, App. A, Rules of Evid., N.J.R.E. 504.

[15] Attorney and Client 45 32(12)

45 Attorney and Client
45I The Office of Attorney
45I(B) Privileges, Disabilities, and Liabilities
45k32 Regulation of Professional Conduct, in General
45k32(12) k. Relations, dealings, or communications with witness, juror, judge, or opponent. Most Cited Cases

E-mail messages exchanged between former employee and her attorneys before employee filed employment discrimination suit against employer, which e-mails were obtained by employer's counsel through legitimate attempt to preserve evidence by retaining a computer forensic expert to retrieve all e-mails that were automatically saved on employer's work-issued laptop computer, were "inadvertently sent" to employer's counsel, for purposes of professional conduct rule requiring a lawyer who received a document and had reasonable cause to believe that the document was inadvertently sent to stop reading the document, promptly notify the sender, and return it to sender; e-mails were exchanged through employee's personal, password-protected, web-based e-mail account, but, without employee's knowledge, browser software made copies of each webpage she viewed. RPC 4.4(b).

[16] Attorney and Client 45 32(12)

45 Attorney and Client
45I The Office of Attorney
45I(B) Privileges, Disabilities, and Liabilities
45k32 Regulation of Professional Conduct, in General
45k32(12) k. Relations, dealings, or communications with witness, juror, judge, or opponent. Most Cited Cases

Employer's counsel, by failing to stop reading e-mail messages, promptly notify employee, and return e-mails to employee, violated professional conduct rule regarding documents inadvertently sent to a lawyer, with respect to e-mail messages exchanged between former employee and her attorneys, on work-issued laptop computer through employee's personal, password-protected, web-based e-mail account, before employee filed employment discrimination suit against employer, though the e-mails had been obtained through a legitimate attempt by employer's counsel to preserve evidence by retaining a computer forensic expert to retrieve all e-mails that were automatically saved on laptop's hard drive in "cache" folder of temporary Internet files. RPC 4.4(b).

[17] Appeal and Error 30 1178(1)

30 Appeal and Error
30XVII Determination and Disposition of Cause
30XVII(D) Reversal
30k1178 Ordering New Trial, and Directing Further Proceedings in Lower Court
30k1178(1) k. In general. Most Cited

Cases

Case would be remanded for hearing to determine what, if any, sanctions should be imposed on employer's counsel for violating professional conduct rule requiring a lawyer who received a document and had reasonable cause to believe that the document was inadvertently sent to stop reading the document, promptly notify the sender, and return it to sender, which violation related to e-mail messages exchanged between former employee and her attorneys before employee filed employment discrimination suit against employer; appellate court could not determine how confidential or critical the messages were, because forensically retrieved version of e-mails submitted to appellate court was not easy to read or fully understand in isolation, and no record had yet been developed about the e-mails' full use. RPC 4.4(b).

[18] Attorney and Client 45 19

45 Attorney and Client
45I The Office of Attorney
45I(B) Privileges, Disabilities, and Liabilities
45k19 k. Disqualification in general. Most Cited Cases

When deciding whether to disqualify counsel, the court should balance competing interests, weighing the need to maintain the highest standards of the profession against a client's right freely to choose his counsel.

****654** Peter G. Verniero, Newark, argued the cause for appellants (Sills Cummis & Gross and Porzio Bromberg & Newman, attorneys; Mr. Verniero and James M. Hirschhorn, of counsel; Mr. Verniero, Mr. Hirschhorn, Lynne Anne Anderson, and Jerrold J. Wohlgemuth, on the briefs).

Peter J. Frazza, Short Hills, argued the cause for respondent (Budd Larner, attorneys; Mr. Frazza and David J. Novack, of counsel; Mr. Frazza, Donald P. Jacobs, and Allen L. Harris, on the briefs).

Marvin M. Goldstein, Newark, submitted a brief on behalf of amicus curiae Employers Association of New Jersey (Proskauer Rose, attorneys; Mr. Goldstein, Mark A. Saloman, and John J. Sarno, of counsel and on the brief).

Jeffrey S. Mandel, Morristown, submitted a brief on behalf of amicus curiae Association of Criminal Defense Lawyers of New Jersey (PinilisHalpern, attorneys).

Richard E. Yaskin, Cherry Hill, submitted a brief on behalf of amicus curiae National Employment Lawyers Association of New Jersey (Mr. Yaskin and Resnick, Nirenberg & Cash, attorneys; Mr. Yaskin and Jonathan I. Nirenberg, on the brief).

Allen A. Etish, President, Haddonfield, submitted a brief on behalf of amicus curiae New Jersey State Bar Association (Mr. Etish, Stryker, Tams & Dill, Gibbons, and Scarinci Hollenbeck, attorneys; Mr. Etish, Douglas S. Brierley, Fruqan Mouzon, and Thomas Hoff Prol, on the brief).

Chief Justice RABNER delivered of the opinion of the Court.

***307** In the past twenty years, businesses and private citizens alike have embraced the use of computers, electronic communication devices, the Internet, and e-mail. As those and other forms of technology ****655** evolve, the line separating business from personal activities can easily blur.

In the modern workplace, for example, occasional, personal use of the Internet is commonplace. Yet that simple act can raise complex issues about an employer's monitoring of the workplace and an employee's reasonable expectation of privacy.

This case presents novel questions about the extent to which an employee can expect privacy and confidentiality in personal e-mails with her attorney, which she accessed on a computer belonging to her employer. Marina Stengart used her company-issued laptop to exchange e-mails with her lawyer through her personal, password-protected, web-based e-mail account. She later filed an employment discrimination lawsuit against her employer, Loving Care Agency, Inc. (Loving Care), and others.

In anticipation of discovery, Loving Care hired a computer forensic expert to recover all files stored on the laptop including the e-mails, which had been automatically saved on the hard drive. Loving Care's attorneys reviewed the e-mails and used information culled from them in the course of discovery. In response, Stengart's lawyer demanded that communications between him and Stengart, which he considered privileged, be identified and returned. Opposing counsel disclosed the documents but maintained that the company had the right to review them. Stengart then sought relief in court.

***308** The trial court ruled that, in light of the company's written policy on electronic communications, Stengart waived the attorney-client privilege by sending e-mails on a company computer. The Appellate Division reversed and found that Loving Care's counsel had violated *RPC* 4.4(b) by reading and using the privileged documents.

We hold that, under the circumstances, Stengart could reasonably expect that e-mail communications with her lawyer through her personal account would remain private, and that sending and receiving them via a company laptop did not eliminate the attorney-client privilege that protected them. By reading e-mails that were at least arguably privileged and failing to notify Stengart promptly about them, Loving Care's counsel breached *RPC* 4.4(b). We therefore modify and affirm the judgment of the Appellate Division and remand to the trial court to determine what, if any, sanctions should be imposed on counsel for Loving Care.

I.

This appeal arises out of a lawsuit that plaintiff-respondent Marina Stengart filed against her former employer, defendant-appellant Loving Care, its owner, and certain board members and officers of the company. She alleges, among other things, constructive discharge because of a hostile work environment, retaliation, and harassment based on gender, religion, and national origin, in violation of the New Jersey Law Against Discrimination, *N.J.S.A.* 10:5–1 to –49. Loving Care denies the allegations and suggests they are an attempt to escape certain restrictive covenants that are the subject of a separate lawsuit.

Loving Care provides home-care nursing and health services. Stengart began working for Loving Care in 1994 and, over time, was promoted to Executive Director of Nursing. The company provided her with a laptop computer to conduct company business. From that laptop, Stengart could send e-mails using her company e-mail address; she could also access the Internet and visit websites through Loving Care's server. Unbeknownst to Stengart, certain browser software in place automatically****656** made a copy ***309** of each web page she viewed, which was then saved on the computer's hard drive in a “cache” folder of temporary Internet files. Unless deleted and overwritten with new data, those temporary Internet files remained on the hard drive.

On several days in December 2007, Stengart used her laptop to access a personal, password-protected e-mail account on Yahoo's website, through which she communicated with her attorney about her situation at work. She never saved her Yahoo ID or password on the company laptop.

Not long after, Stengart left her employment with Loving Care and returned the laptop. On February 7,

2008, she filed the pending complaint.

In an effort to preserve electronic evidence for discovery, in or around April 2008, Loving Care hired experts to create a forensic image of the laptop's hard drive. Among the items retrieved were temporary Internet files containing the contents of seven or eight e-mails Stengart had exchanged with her lawyer via her Yahoo account.[FN1] Stengart's lawyers represented at oral argument that one e-mail was simply a communication he sent to her, to which she did not respond.

FN1. The record does not specify how many of the e-mails were sent or received during work hours. Loving Care asserts that the e-mails in question were exchanged during work hours through the company's server. However, counsel for Stengart represented at oral argument that four of the e-mails were transmitted or accessed during non-work hours—three on a weekend and one on a holiday. It is unclear, and ultimately not relevant, whether Stengart was at the office when she sent or reviewed them.

A legend appears at the bottom of the e-mails that Stengart's lawyer sent. It warns readers that

> THE INFORMATION CONTAINED IN THIS EMAIL COMMUNICATION IS INTENDED ONLY FOR THE PERSONAL AND CONFIDENTIAL USE OF THE DESIGNATED RECIPIENT NAMED ABOVE. This message may be an Attorney–Client communication, and as such is privileged and confidential. If the reader o[FN2]f this message is not the intended recipient, you are hereby notified that ***310** you have received this communication in error, and that your review, dissemination, distribution, or copying of the message is strictly prohibited. If you have received this transmission in error, please destroy this transmission and notify us immediately by telephone and/or reply email.

FN2. In the forensically retrieved version of the e-mails submitted to this Court under seal, the legend is reprinted only up until the location of the footnote in the above text. The retrieved messages also list Stengart's lawyer's full name more than a dozen times and his e-mail address—comprised of the lawyer's first initial, full last name, and the law firm's name—more than three dozen times. Counsel for Loving Care submitted certifications in which they explain that they were aware the e-mails were between Stengart and her lawyer but believed the communications were not protected by the attorney-client privilege for reasons discussed below.

At least two attorneys from the law firm representing Loving Care, Sills Cummis (the "Firm"), reviewed the e-mail communications between Stengart and her attorney. The Firm did not advise opposing counsel about the e-mails until months later. In its October 21, 2008 reply to Stengart's first set of interrogatories, the Firm stated that it had obtained certain information from "e-mail correspondence"—between Stengart and her lawyer—from Stengart's "office computer on December 12, 2007 at 2:25 p.m." In response, Stengart's****657** attorney sent a letter demanding that the Firm identify and return all "attorney-client privileged communications" in its possession. The Firm identified and disclosed the e-mails but asserted that Stengart had no reasonable expectation of privacy in files on a company-owned computer in light of the company's policy on electronic communications.

Loving Care and its counsel relied on an Administrative and Office Staff Employee Handbook that they maintain contains the company's Electronic Communication policy (Policy). The record contains various versions of an electronic communications

policy, and Stengart contends that none applied to her as a senior company official. Loving Care disagrees. We need not resolve that dispute and assume the Policy applies in addressing the issues on appeal.

The proffered Policy states, in relevant part:

> ***311** The company reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the company's media systems and services at any time, with or without notice.
>
> ....
>
> E-mail and voice mail messages, internet use and communication and computer files are considered part of the company's business and client records. Such communications are not to be considered private or personal to any individual employee.
>
> The principal purpose of electronic mail (*e-mail*) is for company business communications. Occasional personal use is permitted; however, the system should not be used to solicit for outside business ventures, charitable organizations, or for any political or religious purpose, unless authorized by the Director of Human Resources.

The Policy also specifically prohibits "[c]ertain uses of the e-mail system" including sending inappropriate sexual, discriminatory, or harassing messages, chain letters, "[m]essages in violation of government laws," or messages relating to job searches, business activities unrelated to Loving Care, or political activities. The Policy concludes with the following warning: "Abuse of the electronic communications system may result in disciplinary action up to and including separation of employment."

Stengart's attorney applied for an order to show cause seeking return of the e-mails and other relief. The trial court converted the application to a motion, which it later denied in a written opinion. The trial court concluded that the Firm did not breach the attorney-client privilege because the company's Policy placed Stengart on sufficient notice that her e-mails would be considered company property. Stengart's request to disqualify the Firm was therefore denied.

The Appellate Division granted Stengart's motion for leave to appeal. The panel reversed the trial court order and directed the Firm to turn over all copies of the e-mails and delete any record of them. *Stengart v. Loving Care Agency, Inc.*, 408 *N.J.Super.* 54, 973 *A.*2d 390 (App.Div.2009). Assuming that the Policy applied to Stengart, the panel found that "[a]n objective reader could reasonably conclude ... that not all personal emails are necessarily company property." *Id.* at 64, 973 *A.*2d 390. In other words, an employee could "retain an expectation of privacy" in personal e-mails sent on ***312** a company computer given the language of the Policy. *Id.* at 65, 973 *A.*2d 390.

The panel balanced Loving Care's right to enforce reasonable rules for the workplace against the public policies underlying the attorney-client privilege. *Id.* at 66, 973 *A.*2d 390. The court rejected the notion ****658** that "ownership of the computer [is] the sole determinative fact" at issue and instead explained that there must be a nexus between company policies and the employer's legitimate business interests. *Id.* at 68–69, 973 *A.*2d 390. The panel concluded that society's important interest in shielding communications with an attorney from disclosure outweighed the company's interest in upholding the Policy. *Id.* at 74–75, 973 *A.*2d 390. As a result, the panel found that the e-mails were protected by the attorney-client privilege and should be returned. *Id.* at 75, 973 *A.*2d 390.

The Appellate Division also concluded that the Firm breached its obligations under *RPC* 4.4(b) by failing to alert Stengart's attorneys that it possessed the e-mails before reading them. The panel remanded for a hearing to determine whether disqualification of the Firm or some other sanction was appropriate.

We granted Loving Care's motion for leave to appeal and ordered a stay pending the outcome of this appeal.

II.

Loving Care argues that its employees have no expectation of privacy in their use of company computers based on the company's Policy. In its briefs before this Court, the company also asserts that by accessing e-mails on a personal account through Loving Care's computer and server, Stengart either prevented any attorney-client privilege from attaching or waived the privilege by voluntarily subjecting her e-mails to company scrutiny. Finally, Loving Care maintains that its counsel did not violate *RPC* 4.4(b) because the e-mails were left behind on Stengart's company computer—not "inadvertently sent," as per the *Rule*—and the ***313** Firm acted in the good faith belief that any privilege had been waived.

Stengart argues that she intended the e-mails with her lawyer to be confidential and that the Policy, even if it applied to her, failed to provide adequate warning that Loving Care would save on a hard drive, or monitor the contents of, e-mails sent from a personal account. Stengart also maintains that the communications with her lawyer were privileged. When the Firm encountered the arguably protected e-mails, Stengart contends it should have immediately returned them or sought judicial review as to whether the attorney-client privilege applied.

We granted amicus curiae status to the following organizations: the Employers Association of New Jersey (EANJ), the National Employment Lawyers Association of New Jersey (NELA–NJ), the Association of Criminal Defense Lawyers of New Jersey (ACDL–NJ), and the New Jersey State Bar Association (NJSBA).

EANJ calls for reversal of the Appellate Division decision. It notes the dramatic, recent increase in the use of non-business-related e-mails at work and submits that, by allowing occasional personal use of company property as a courtesy to employees, companies do not create a reasonable expectation of privacy in the use of their computer systems. EANJ also contends that the Appellate Division's analysis—particularly, its focus on whether workplace policies in the area of electronic communications further legitimate business interests—will unfairly burden employers and undermine their ability to protect corporate assets.

NELA–NJ and ACDL–NJ support the Appellate Division's ruling. NELA–NJ submits that an employee has a substantive right to privacy in her password-protected e-mails, even if accessed from an employer-owned computer, and that an employer's invasion of that privacy right must be narrowly tailored to the employer's****659** legitimate business interests. ACDL–NJ adds that the need to shield private communications from disclosure is amplified when the attorney-client privilege is at stake.

***314** NJSBA expresses concern about preserving the attorney-client privilege in the "increasingly technology-laden world" in which attorneys practice. NJSBA cautions against allowing inadvertent or casual waivers of the privilege. To analyze the competing interests presented in cases like this, NJSBA suggests various factors that courts should consider in deciding whether the privilege has been waived.

III.

Our analysis draws on two principal areas: the adequacy of the notice provided by the Policy and the important public policy concerns raised by the attorney-client privilege. Both inform the reasonableness of an employee's expectation of privacy in this matter. We address each area in turn.

A.

We start by examining the meaning and scope of the Policy itself. The Policy specifically reserves to Loving Care the right to review and access "all matters on the company's media systems and services at any time." In addition, e-mail messages are plainly "considered part of the company's business ... records."

It is not clear from that language whether the use of personal, password-protected, web-based e-mail accounts via company equipment is covered. The Policy uses general language to refer to its "media systems and services" but does not define those terms. Elsewhere, the Policy prohibits certain uses of "the e-mail system," which appears to be a reference to company e-mail accounts. The Policy does not address personal accounts at all. In other words, employees do not have express notice that messages sent or received on a personal, web-based e-mail account are subject to monitoring if company equipment is used to access the account.

***315** The Policy also does not warn employees that the contents of such e-mails are stored on a hard drive and can be forensically retrieved and read by Loving Care.

The Policy goes on to declare that e-mails "are not to be considered private or personal to any individual employee." In the very next point, the Policy acknowledges that "[o]ccasional personal use [of e-mail] is permitted." As written, the Policy creates ambiguity about whether personal e-mail use is company or private property.

The scope of the written Policy, therefore, is not entirely clear.

B.

[1] The policies underlying the attorney-client privilege further animate this discussion. The venerable privilege is enshrined in history and practice. *Fellerman v. Bradley,* 99 *N.J.* 493, 498, 493 *A.*2d 1239 (1985) ("[T]he attorney-client privilege is recognized as one of 'the oldest of the privileges for confidential communications.' ") (quoting 8 J. Wigmore, *Evidence* § 2290, at 542 (McNaughton rev.1961)). Its primary rationale is to encourage "free and full disclosure of information from the client to the attorney." *Ibid.* That, in turn, benefits the public, which "is well served by sound legal counsel" based on full, candid, and confidential exchanges. *Id.* at 502, 493 *A.*2d 1239.

The privilege is codified at *N.J.S.A.* 2A:84A–20, and it appears in the *Rules of Evidence* as *N.J.R.E.* 504. Under the *Rule,* "[f]or a communication to be privileged it must initially be expressed by an individual in his capacity as a client in ****660** conjunction with seeking or receiving legal advice from the attorney in his capacity as such, with the expectation that its content remain confidential." *Fellerman, supra,* 99 *N.J.* at 499, 493 *A.*2d 1239 (citing *N.J.S.A.* 2A:84A–20(1) and (3)).

[2] E-mail exchanges are covered by the privilege like any other form of communication. *See Seacoast Builders Corp. v. Rutgers,* 358 *N.J.Super.* 524, 553, 818 *A.*2d 455 (App.Div.2003) ***316** (finding e-mail from client to attorney "obviously protected by the attorney-client privilege as a communication with counsel in the course of a professional relationship and in confidence").

The e-mail communications between Stengart and her lawyers contain a standard warning that their contents are personal and confidential and may constitute attorney-client communications. The subject matter of those messages appears to relate to Stengart's working conditions and anticipated lawsuit against Loving Care.

IV.

Under the particular circumstances presented, how should a court evaluate whether Stengart had a reasonable expectation of privacy in the e-mails she

exchanged with her attorney?

A.

[3] Preliminarily, we note that the reasonable-expectation-of-privacy standard used by the parties derives from the common law and the Search and Seizure Clauses of both the Fourth Amendment and Article I, paragraph 7 of the New Jersey Constitution The latter sources do not apply in this case, which involves conduct by private parties only.[FN3]

FN3. In addition, a right to privacy can be found in Article I, paragraph 1 of the New Jersey Constitution. *Hennessey v. Coastal Eagle Point Oil Co.*, 129 *N.J.* 81, 95–96, 609 *A.*2d 11 (1992).

[4][5] The common law source is the tort of "intrusion on seclusion," which can be found in the *Restatement (Second) of Torts* § 652B (1977). That section provides that "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." *Restatement, supra*, § 652B. A high threshold must be cleared to assert a ***317** cause of action based on that tort. *Hennessey, supra*, 129 *N.J.* at 116, 609 *A.*2d 11 (Pollock, J., concurring). A plaintiff must establish that the intrusion "would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object." *Restatement, supra*, § 652B cmt. d.

[6][7] As is true in Fourth Amendment cases, the reasonableness of a claim for intrusion on seclusion has both a subjective and objective component. *See State v. Sloane*, 193 *N.J.* 423, 434, 939 *A.*2d 796 (2008) (analyzing Fourth Amendment); *In re Asia Global Crossing, Ltd.*, 322 *B.R.* 247, 257 (Bankr.S.D.N.Y.2005) (analyzing common law tort). Moreover, whether an employee has a reasonable expectation of privacy in her particular work setting "must be addressed on a case-by-case basis." *O'Connor v. Ortega*, 480 *U.S.* 709, 718, 107 *S.Ct.* 1492, 1498, 94 *L.Ed.*2d 714, 723 (1987) (plurality opinion) (reviewing public sector employment).

B.

A number of courts have tested an employee's claim of privacy in files stored on ****661** company computers by evaluating the reasonableness of the employee's expectation. No reported decisions in New Jersey offer direct guidance for the facts of this case.[FN4] In one matter, *State v. M.A.*, 402 *N.J.Super.* 353, 954 *A.*2d 503 (App.Div.2008), the Appellate Division found that the defendant had no reasonable expectation of privacy in personal information he stored on a workplace computer under a separate password. *Id.* at 369, 954 *A.*2d 503. The defendant had been advised that all computers were company property. *Id.* at 359, 954 *A.*2d 503. His former employer consented to a search by the State Police, who, in turn, retrieved information tied to the theft of company funds. *Id.* at 361–62, 954 *A.*2d 503. The court reviewed the search in the context of the Fourth Amendment and found no basis for the ***318** defendant's privacy claim in the contents of a company computer that he used to commit a crime. *Id.* at 365–69, 954 *A.*2d 503.

FN4. Under our rules, unpublished opinions do not constitute precedent and "are not to be cited by any court." *R.* 1:36–3. As a result, we do not address any unpublished decisions raised by the parties.

Doe v. XYC Corp., 382 *N.J.Super.* 122, 887 *A.*2d 1156 (App.Div.2005), likewise did not involve attorney-client e-mails. In *XYC Corp.*, the Appellate Division found no legitimate expectation of privacy in an employee's use of a company computer to access websites containing adult and child pornography. *Id.* at 139, 887 *A.*2d 1156. In its analysis, the court referenced a policy authorizing the company to monitor

employee website activity and e-mails, which were deemed company property. *Id.* at 131, 138–39, 887 *A.*2d 1156.

Certain decisions from outside New Jersey, which the parties also rely on, are more instructive. Among them, *National Economic Research Associates v. Evans,* 21 *Mass. L. Rptr.* No. 15, at 337, 2006 WL 2440008 (Mass.Super.Ct. Aug. 3, 2006), is most analogous to the facts here. In *Evans,* an employee used a company laptop to send and receive attorney-client communications by e-mail. In doing so, he used his personal, password-protected Yahoo account and not the company's e-mail address. *Ibid.* The e-mails were automatically stored in a temporary Internet file on the computer's hard drive and were later retrieved by a computer forensic expert.*Ibid.* The expert recovered various attorney-client e-mails; at the instruction of the company's lawyer, those e-mails were not reviewed pending guidance from the court. *Ibid.*

A company manual governed the laptop's use. The manual permitted personal use of e-mail, to "be kept to a minimum," but warned that computer resources were the "property of the Company" and that e-mails were "not confidential" and could be read "during routine checks." *Id.* at 338.

The court denied the company's application to allow disclosure of the e-mails that its expert possessed. *Id.* at 337. The court reasoned,

> Based on the warnings furnished in the Manual, Evans [(the employee)] could not reasonably expect to communicate in confidence with his private attorney if Evans ***319** e-mailed his attorney using his NERA [(company)] e-mail address through the NERA Intranet, because the Manual plainly warned Evans that e-mails on the network could be read by NERA network administrators. The Manual, however, did not expressly declare that it would monitor the *content* of Internet communications.... Most importantly, the Manual did not expressly declare, or even implicitly suggest, that NERA would monitor the content****662** of e-mail communications made from an employee's personal e-mail account via the Internet whenever those communications were viewed on a NERA-issued computer. Nor did NERA warn its employees that the content of such Internet e-mail communications is stored on the hard disk of a NERA-issued computer and therefore capable of being read by NERA.
>
> [*Id.* at 338–39.]

As a result, the court found the employee's expectation of privacy in e-mails with his attorney to be reasonable. *Id.* at 339.

In *Asia Global, supra,* the Bankruptcy Court for the Southern District of New York considered whether a bankruptcy trustee could force the production of e-mails sent by company employees to their personal attorneys on the *company's* e-mail system. 322 *B.R.* at 251–52. The court developed a four-part test to "measure the employee's expectation of privacy in his computer files and e-mail":

> (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?
>
> [*Id.* at 257.]

Because the evidence was "equivocal" about the existence of a corporate policy banning personal use of e-mail and allowing monitoring, the court could not conclude that the employees' use of the company e-mail system eliminated any applicable attor-

ney-client privilege. *Id.* at 259–61.

Both *Evans* and *Asia Global* referenced a formal ethics opinion by the American Bar Association that noted "lawyers have a reasonable expectation of privacy when communicating by e-mail maintained by an [online service provider]." *See id.* at 256 (citing ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 413 (1999)); *Evans, supra*, 21 *Mass. L. Rptr.* No. 15, at 339 (same).

***320** Other courts have measured the factors outlined in *Asia Global* among other considerations. In reviewing those cases, we are mindful of the fact-specific nature of the inquiry involved and the multitude of different facts that can affect the outcome in a given case. No one factor alone is necessarily dispositive.

According to some courts, employees appear to have a lesser expectation of privacy when they communicate with an attorney using a company e-mail system as compared to a personal, web-based account like the one used here. *See, e.g., Smyth v. Pillsbury Co.*, 914 *F.Supp.* 97, 100–01 (E.D.Pa.1996) (finding no reasonable expectation of privacy in unprofessional e-mails sent to supervisor through internal corporate e-mail system); *Scott v. Beth Israel Med. Ctr., Inc.*, 17 *Misc.*3d 934, 847 *N.Y.S.*2d 436, 441–43 (N.Y.Sup.Ct.2007) (finding no expectation of confidentiality when company e-mail used to send attorney-client messages). *But see Convertino v. U.S. Dep't of Justice*, 674 *F.Supp.2d* 97, 110 (D.D.C.2009) (finding reasonable expectation of privacy in attorney-client e-mails sent via employer's e-mail system). As a result, courts might treat e-mails transmitted via an employer's e-mail account differently than they would web-based e-mails sent on the same company computer.

Courts have also found that the existence of a clear company policy banning personal e-mails can also diminish the reasonableness of an employee's claim to privacy in e-mail messages with his or her attorney. *Compare* ****663***Scott, supra*, 847 *N.Y.S.*2d at 441 (finding e-mails sent to attorney not privileged and noting that company's e-mail policy prohibiting personal use was "critical to the outcome"), *with Asia Global, supra*, 322 *B.R.* at 259–61 (declining to find e-mails to attorney were not privileged in light of unclear evidence as to existence of company policy banning personal e-mail use). We recognize that a zero-tolerance policy can be unworkable and unwelcome in today's dynamic and mobile workforce and do not seek to encourage that approach in any way.

The location of the company's computer may also be a relevant consideration. In ***321***Curto v. Medical World Communications, Inc.*, 99 *Fair Empl. Prac. Cas.* (BNA) 298, 2006 WL 1318387 (E.D.N.Y. May 15, 2006), for example, an employee working from a home office sent e-mails to her attorney on a company laptop via her personal AOL account. *Id.* at 301. Those messages did not go through the company's servers but were nonetheless retrievable. *Ibid.* Notwithstanding a company policy banning personal use, the trial court found that the e-mails were privileged. *Id.* at 305.

We realize that different concerns are implicated in cases that address the reasonableness of a privacy claim under the Fourth Amendment. *See, e.g., O'Connor, supra*, 480 *U.S.* at 714–19, 107 *S.Ct.* at 1496–98, 94 *L.Ed.*2d at 721–24 (discussing whether public hospital's search of employee workplace violated employee's expectation of privacy under Fourth Amendment); *United States v. Simons*, 206 *F.*3d 392, 397–98 (4th Cir.2000) (involving search warrants for work computer of CIA employee, which revealed more than fifty pornographic images of minors); *M.A., supra*, 402 *N.J.Super.* at 366–69, 954 *A.*2d 503 (involving Fourth Amendment analysis of State Police search of employee's computer, resulting in theft charges). This case, however, involves no governmental action. Stengart's relationship with her private

employer does not raise the specter of any government official unreasonably invading her rights.

V.

A.

[8] Applying the above considerations to the facts before us, we find that Stengart had a reasonable expectation of privacy in the e-mails she exchanged with her attorney on Loving Care's laptop.

Stengart plainly took steps to protect the privacy of those e-mails and shield them from her employer. She used a personal, password-protected e-mail account instead of her company e-mail address and did not save the account's password on her computer. In other words, she had a subjective expectation of privacy in ***322** messages to and from her lawyer discussing the subject of a future lawsuit.

[9] In light of the language of the Policy and the attorney-client nature of the communications, her expectation of privacy was also objectively reasonable. As noted earlier, the Policy does not address the use of personal, web-based e-mail accounts accessed through company equipment. It does not address personal accounts at all. Nor does it warn employees that the contents of e-mails sent via personal accounts can be forensically retrieved and read by the company. Indeed, in acknowledging that occasional personal use of e-mail is permitted, the Policy created doubt about whether those e-mails are company or private property.

Moreover, the e-mails are not illegal or inappropriate material stored on Loving Care's equipment, which might harm the company in some way. *See* ****664***Muick v. Glenayre Elecs.*, 280 *F.*3d 741, 742–43 (7th Cir.2002); *Smyth, supra*, 914 *F.Supp.* at 98, 101; *XYC Corp., supra*, 382 *N.J.Super.* at 136–40, 887 *A.*2d 1156. They are conversations between a lawyer and client about confidential legal matters, which are historically cloaked in privacy. Our system strives to keep private the very type of conversations that took place here in order to foster probing and honest exchanges.

In addition, the e-mails bear a standard hallmark of attorney-client messages. They warn the reader directly that the e-mails are personal, confidential, and may be attorney-client communications. While a pro forma warning at the end of an e-mail might not, on its own, protect a communication, *see Scott, supra*, 847 *N.Y.S.*2d at 444, other facts present here raise additional privacy concerns.

Under all of the circumstances, we find that Stengart could reasonably expect that e-mails she exchanged with her attorney on her personal, password-protected, web-based e-mail account, accessed on a company laptop, would remain private.

***323** [10] It follows that the attorney-client privilege protects those e-mails. *See Asia Global, supra*, 322 *B.R.* at 258–59 (noting "close correlation between the objectively reasonable expectation of privacy and the objective reasonableness of the intent that a communication between a lawyer and a client was given in confidence"). In reaching that conclusion, we necessarily reject Loving Care's claim that the attorney-client privilege either did not attach or was waived. In its reply brief and at oral argument, Loving Care argued that the manner in which the e-mails were sent prevented the privilege from attaching. Specifically, Loving Care contends that Stengart effectively brought a third person into the conversation from the start—watching over her shoulder—and thereby forfeited any claim to confidentiality in her communications. We disagree.

Stengart has the right to prevent disclosures by third persons who learn of her communications "in a manner not reasonably to be anticipated." *See N.J.R.E.* 504(1)(c)(ii). That is what occurred here. The Policy did not give Stengart, or a reasonable person in her

position, cause to anticipate that Loving Care would be peering over her shoulder as she opened e-mails from her lawyer on her personal, password-protected Yahoo account. *See Evans, supra*, 21 *Mass. L. Rptr.* No. 15, at 339. The language of the Policy, the method of transmittal that Stengart selected, and the warning on the e-mails themselves all support that conclusion.

[11][12] Loving Care also argued in earlier submissions that Stengart waived the attorney-client privilege. For similar reasons, we again disagree.

A person waives the privilege if she, "without coercion and with knowledge of [her] right or privilege, made disclosure of any part of the privileged matter or consented to such a disclosure made by anyone." *N.J.R.E.* 530 (codifying *N.J.S.A.* 2A:84A–29). Because consent is not applicable here, we look to whether Stengart either knowingly disclosed the information contained in the e-mails or failed to "take reasonable steps to insure and maintain their ***324** confidentiality." [FN5] ****665***Trilogy Commc'ns, supra*, 279 *N.J.Super.* at 445–48, 652 *A.*2d 1273.

FN5. Because Stengart's conduct satisfies both standards, we need not choose which one governs. *See Kinsella v. NYT Television*, 370 *N.J.Super.* 311, 317–18, 851 *A.*2d 105 (App.Div.2004) (noting "different approaches to determining whether the inadvertent disclosure of privileged materials results in a waiver" without adopting global rule) (citing *Seacoast, supra*, 358 *N.J.Super.* at 550–51, 818 *A.*2d 455 and *State v. J.G.*, 261 *N.J.Super.* 409, 419–20, 619 *A.*2d 232 (App.Div.1993)); *see also Trilogy Commc'ns, Inc. v. Excom Realty, Inc.*, 279 *N.J.Super.* 442, 445–48, 652 *A.*2d 1273 (Law Div.1994) (finding attorney's "[i]nadvertent disclosure through mere negligence should not be deemed to abrogate the attorney-client privilege").

As discussed previously, Stengart took reasonable steps to keep discussions with her attorney confidential: she elected not to use the company e-mail system and relied on a personal, password-protected, web-based account instead. She also did not save the password on her laptop or share it in some other way with Loving Care.

As to whether Stengart knowingly disclosed the e-mails, she certified that she is unsophisticated in the use of computers and did not know that Loving Care could read communications sent on her Yahoo account. Use of a company laptop alone does not establish that knowledge. Nor does the Policy fill in that gap. Under the circumstances, we do not find either a knowing or reckless waiver.

B.

[13][14] Our conclusion that Stengart had an expectation of privacy in e-mails with her lawyer does not mean that employers cannot monitor or regulate the use of workplace computers. Companies can adopt lawful policies relating to computer use to protect the assets, reputation, and productivity of a business and to ensure compliance with legitimate corporate policies. And employers can enforce such policies. They may discipline employees and, when appropriate, terminate them, for violating proper workplace rules that are not inconsistent with a clear mandate of ***325** public policy. *See Hennessey, supra*, 129 *N.J.* at 99–100, 609 *A.*2d 11; *Woolley v. Hoffmann–LaRoche, Inc.*, 99 *N.J.* 284, 290–92, 491 *A.*2d 1257 (1985); *Pierce v. Ortho Pharm. Corp.*, 84 *N.J.* 58, 72–73, 417 *A.*2d 505 (1980). For example, an employee who spends long stretches of the workday getting personal, confidential legal advice from a private lawyer may be disciplined for violating a policy permitting only occasional personal use of the Internet. But employers have no need or basis to read the specific *contents* of personal, privileged, attorney-client communications in order to enforce corporate policy. Because of the important public policy concerns underlying the at-

torney-client privilege, even a more clearly written company manual—that is, a policy that banned all personal computer use and provided unambiguous notice that an employer could retrieve and read an employee's attorney-client communications, if accessed on a personal, password-protected e-mail account using the company's computer system—would not be enforceable.

VI.

We next examine whether the Firm's review and use of the privileged e-mails violated *RPC* 4.4(b). The *Rule* provides that "[a] lawyer who receives a document and has reasonable cause to believe that the document was inadvertently sent shall not read the document or, if he or she has begun to do so, shall stop reading the document, promptly notify the sender, and return the document to the sender." According to the ABA Model Rules on which *RPC* 4.4(b) is patterned, the term " 'document' includes e-mail or other electronic modes of transmission subject to being read or put into readable form." *Model Rules of Prof'l Conduct R.* 4.4 cmt. 2 (2004).

[15] Loving Care contends that the *Rule* does not apply because Stengart left ****666** the e-mails behind on her laptop and did not send them inadvertently. In actuality, the Firm retained a computer forensic expert to retrieve e-mails that were automatically saved on the laptop's hard drive in a "cache" folder of temporary ***326** Internet files. Without Stengart's knowledge, browser software made copies of each webpage she viewed. Under those circumstances, it is difficult to think of the e-mails as items that were simply left behind. We find that the Firm's review of privileged e-mails between Stengart and her lawyer, and use of the contents of at least one e-mail in responding to interrogatories, fell within the ambit of *RPC* 4.4(b) and violated that rule.

[16] To be clear, the Firm did not hack into plaintiff's personal account or maliciously seek out attorney-client documents in a clandestine way. Nor did it rummage through an employee's personal files out of idle curiosity. Instead, it legitimately attempted to preserve evidence to defend a civil lawsuit. Its error was in not setting aside the arguably privileged messages once it realized they were attorney-client communications, and failing either to notify its adversary or seek court permission before reading further. There is nothing in the record before us to suggest any bad faith on the Firm's part in reading the Policy as it did. Nonetheless, the Firm should have promptly notified opposing counsel when it discovered the nature of the e-mails. [FN6]

FN6. The Firm argues that its position was vindicated by the trial court's ruling that the e-mails were not protected by the attorney-client privilege. That argument lacks merit. Stengart still had the right to appeal the trial court's ruling, as she did.

[17][18] The Appellate Division remanded to the trial court to determine the appropriate remedy. It explained that a hearing was needed in that regard to consider

> the content of the emails, whether the information contained in the emails would have inevitably been divulged in discovery that would have occurred absent [the Firm's] knowledge of the emails' content, and the nature of the issues that have been or may in the future be pled in either this or the related Chancery action.
>
> [*Stengart, supra,* 408 *N.J.Super.* at 76–77, 973 *A.*2d 390.]

We agree. The forensically retrieved version of the e-mails submitted to the Court is not easy to read or fully understand in isolation, and no record has yet been developed about the e-mails' full use. For the same reason, we cannot determine how confidential***327** or critical the messages are. In deciding what

sanctions to impose, the trial court should evaluate the seriousness of the breach in light of the specific nature of the e-mails, the manner in which they were identified, reviewed, disseminated, and used, and other considerations noted by the Appellate Division. As to plaintiff's request for disqualification, the court should also "balance competing interests, weighing the 'need to maintain the highest standards of the profession' against 'a client's right freely to choose his counsel.' " *Dewey v. R.J. Reynolds Tobacco Co.*, 109 *N.J.* 201, 218, 536 *A.*2d 243 (1988) (quoting *Gov't of India v. Cook Indus., Inc.*, 569 *F.*2d 737, 739 (2d Cir.1978)).

We leave to the trial court to decide whether disqualification of the Firm, screening of attorneys, the imposition of costs, or some other remedy is appropriate. Under the circumstances, we do not believe a remand to the Chancery judge is required; the matter may proceed before the Law Division judge assigned to the case.

****667** VII.

For the reasons set forth above, we modify and affirm the judgment of the Appellate Division and remand to the trial court for further proceedings.

For affirmance as modification/remandment—Chief Justice RABNER and Justices LONG, LaVECCHIA, ALBIN, WALLACE, RIVERA–SOTO and HOENS—7.
Opposed—None.

N.J.,2010.
Stengart v. Loving Care Agency, Inc.
201 N.J. 300, 990 A.2d 650, 108 Fair Empl.Prac.Cas. (BNA) 1558, 93 Empl. Prac. Dec. P 43,853, 30 IER Cases 873

END OF DOCUMENT

587 F.Supp.2d 548
(Cite as: 587 F.Supp.2d 548)

United States District Court,
S.D. New York.
PURE POWER BOOT CAMP, et al., Plaintiffs,
v.
WARRIOR FITNESS BOOT CAMP, et al., Defendants.

No. 08 Civ. 4810(JGK).
Oct. 23, 2008.

Background: Former employer brought action seeking an injunction and damages, accusing former employee of stealing employer's business model, customers, and internal documents, breaching employee fiduciary duties, and infringing employer's trademarks, trade-dress, and copyrights. Employee filed motion to preclude the use or disclosure of thirty-four of employee's e-mails, obtained by employer.

Holdings: In adopting report and recommendation of United States Magistrate Judge Theodore H. Katz, the District Court, John G. Koeltl, J., held that:
(1) employer's access of employee's personal e-mails, which were stored and accessed directly from accounts maintained by outside electronic communication service provider, was unauthorized, and thus violated Stored Communications Act (SCA);
(2) crime-fraud exception to attorney-client privilege was not applicable; and
(3) as a sanction for employer's violations of SCA, court would preclude employer from admitting e-mails as evidence, however, such evidence could be used for impeachment purposes should employee open the door.

Order in accordance with opinion.

West Headnotes

[1] Telecommunications 372 1439

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General
372k1435 Acts Constituting Interception or Disclosure
372k1439 k. Computer communications. Most Cited Cases

A person violates the Stored Communications Act (SCA) if she accesses an electronic communication service, or obtains an electronic communication while it is still in electronic storage, without authorization. 18 U.S.C.A. § 2701.

[2] Telecommunications 372 1439

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General
372k1435 Acts Constituting Interception or Disclosure
372k1439 k. Computer communications. Most Cited Cases

Unauthorized access to e-mails that had previously been sent or received did not constitute an “interception” of an electronic communication under the Electronic Communications Privacy Act (ECPA). 18 U.S.C.A. §§ 2510, 2511.

[3] Action 13 3

13 Action

13I Grounds and Conditions Precedent
13k3 k. Statutory rights of action. Most Cited Cases

Criminal Law 110 392.21

110 Criminal Law
110XVII Evidence
110XVII(I) Competency in General
110k392.1 Wrongfully Obtained Evidence
110k392.21 k. Electronic surveillance; telecommunications. Most Cited Cases
(Formerly 110k394.3)

Telecommunications 372 1443

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General
372k1442 Actions
372k1443 k. In general. Most Cited Cases

New York rule prohibiting admission of evidence obtained by eavesdropping does not provide a separate civil cause of action, but, rather, is only a vehicle through which evidence may be excluded in an underlying case; rule also does not provide for damages, attorney fees, costs, or any remedy other than exclusion of the evidence. N.Y.McKinney's CPLR 4506.

[4] Telecommunications 372 1439

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General
372k1435 Acts Constituting Interception or Disclosure
372k1439 k. Computer communications. Most Cited Cases

Employer's access of employee's personal e-mails, which were stored and accessed directly from accounts maintained by outside electronic communication service provider, was unauthorized, and thus violated Stored Communications Act (SCA); employee, who did not store any of those communications on the employer's computers, servers, or systems and who did not send or receive such communications through the company e-mail system or computer, had a reasonable expectation of privacy in his personal e-mail accounts, which were protected by passwords, since nothing in employer's policy even suggested that if an employee simply viewed a single, personal e-mail from a third party e-mail provider, over employer's computers, then all of the his personal e-mails on whatever personal e-mail accounts he used, would be subject to inspection, and employee did not give implied consent to search his e-mails by leaving his login information stored on employer's computers where it could be discovered and used by employer. 18 U.S.C.A. § 2701.

[5] Privileged Communications and Confidentiality 311H 102

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk102 k. Elements in general; definition. Most Cited Cases
(Formerly 410k198(1))

Attorney-client privilege affords confidentiality to communications among clients and their attorneys, for the purpose of seeking and rendering an opinion on law or legal services, or assistance in some legal proceeding, so long as the communications were intended to be, and were in fact, kept confidential.

[6] Privileged Communications and Confidentiality 311H 129

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk128 Professional Character of Employment or Transaction
311Hk129 k. In general. Most Cited Cases
(Formerly 410k200)

Privileged Communications and Confidentiality 311H 130

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk128 Professional Character of Employment or Transaction
311Hk130 k. Business communications. Most Cited Cases
(Formerly 410k200)

In order to merit protection under attorney-client privilege, the "predominant purpose" of the communication must be to render or solicit legal advice, as opposed to business or policy advice.

[7] Privileged Communications and Confidentiality 311H 173

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk171 Evidence
311Hk173 k. Presumptions and burden of proof. Most Cited Cases
(Formerly 410k222)

Burden of establishing the existence of an attorney-client privilege, in all of its elements, rests with the party asserting it.

[8] Privileged Communications and Confidentiality 311H 168

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk168 k. Waiver of privilege. Most Cited Cases
(Formerly 410k219(3))

Attorney-client privilege is waived if the holder of the privilege voluntarily discloses or consents to disclosure of any significant part of the communication to a third party or stranger to the attorney-client relationship.

[9] Privileged Communications and Confidentiality 311H 168

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk168 k. Waiver of privilege. Most Cited Cases
(Formerly 410k219(3))

A party who seeks to uphold attorney-client privilege must take affirmative measures to maintain the confidentiality of attorney-client communications.

[10] Privileged Communications and Confidentiality 311H 141

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk135 Mode or Form of Communications
311Hk141 k. E-mail and electronic communication. Most Cited Cases
(Formerly 410k204(2))

Fact that e-mails sent by paralegal to law firm's client contained a warning indicating that they contained "PRIVILEGED AND CONFIDENTIAL INFORMATION," did not transform them from non-privileged communications into communications protected by attorney-client privilege.

[11] Privileged Communications and Confiden-

tiality 311H 141

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk135 Mode or Form of Communications
311Hk141 k. E-mail and electronic communication. Most Cited Cases
(Formerly 410k204(2))

A privileged communication does not lose its protection under New York's attorney-client privilege for the sole reason it was sent by e-mail. N.Y.C.P.L.R. 4548.

[12] Privileged Communications and Confidentiality 311H 154

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk154 k. Criminal or other wrongful act or transaction; crime-fraud exception. Most Cited Cases
(Formerly 410k201(2))

A party wishing to invoke the crime-fraud exception to attorney-client privilege must demonstrate that there is a factual basis for a showing of probable cause to believe that a fraud or crime has been committed and that the communications in question were in furtherance of the fraud or crime; it is not enough to show merely that privileged communications might provide evidence of a crime or fraud; rather, the communication itself must have been in furtherance of a fraud or crime and must have been intended to facilitate the fraud or crime.

[13] Privileged Communications and Confidentiality 311H 154

311H Privileged Communications and Confidentiality
311HIII Attorney-Client Privilege
311Hk154 k. Criminal or other wrongful act or transaction; crime-fraud exception. Most Cited Cases
(Formerly 410k201(2))

Fact that communication between attorney and client arose in the larger context of client's attempt to set up a competing business, and discussed matters which might, in client's former employer's eyes, constitute past criminal or fraudulent actions, did not transform the communication into one which furthered a crime or fraud so as to fall within crime-fraud exception to attorney-client privilege.

[14] Telecommunications 372 1439

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General
372k1435 Acts Constituting Interception or Disclosure
372k1439 k. Computer communications. Most Cited Cases

Crime-fraud exception to attorney-client privilege does not excuse violations of the Stored Communications Act (SCA). 18 U.S.C.A. § 2701.

[15] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

"Spoliation" is the destruction or significant alteration of evidence, or failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation.

587 F.Supp.2d 548
(Cite as: 587 F.Supp.2d 548)

[16] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

When the nature of the breach of litigant's duty is non-production of evidence, as opposed to actual destruction or significant alteration, a district court has broad discretion in fashioning an appropriate sanction; harm caused by delay in production is a relevant factor in determining sanctions, if a court determines that sanctions are warranted.

[17] Federal Civil Procedure 170A 1636.1

170A Federal Civil Procedure
170AX Depositions and Discovery
170AX(E) Discovery and Production of Documents and Other Tangible Things
170AX(E)5 Compliance; Failure to Comply
170Ak1636 Failure to Comply; Sanctions
170Ak1636.1 k. In general. Most Cited Cases

Plaintiffs's obscuring print dates of e-mails did not amount to spoliation warranting the imposition of sanctions, let alone total preclusion where defendants were not harmed by the delay, as they were not prevented from addressing the evidence or making any arguments related to the e-mails.

[18] Federal Civil Procedure 170A 2757

170A Federal Civil Procedure
170AXX Sanctions
170AXX(A) In General
170Ak2756 Authority to Impose
170Ak2757 k. Inherent authority. Most Cited Cases

Federal courts have inherent equitable powers of courts of law over their own process, to prevent abuses, oppression, and injustices.

[19] Federal Civil Procedure 170A 2757

170A Federal Civil Procedure
170AXX Sanctions
170AXX(A) In General
170Ak2756 Authority to Impose
170Ak2757 k. Inherent authority. Most Cited Cases

Federal courts may impose sanctions and rely upon their inherent authority even where the conduct at issue is not covered by one of the other sanctioning provisions; furthermore, a district court may resort to its inherent power to fashion sanctions, even in situations similar or identical to those contemplated by a statute or rule.

[20] Telecommunications 372 1439

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(A) In General
372k1435 Acts Constituting Interception or Disclosure
372k1439 k. Computer communications. Most Cited Cases

Witnesses 410 331.5

410 Witnesses
410IV Credibility and Impeachment
410IV(A) In General
410k331.5 k. Competency of impeaching evidence in general. Most Cited Cases

Pursuant to its inherent equitable powers, and in order to protect the integrity of the judicial process, court, as a sanction for employer's violations of Stored Communications Act (SCA) by accessing employee's personal e-mails in bad faith, would preclude employer from admitting those e-mails as evidence in its suit against former employee, but such evidence could be used for impeachment purposes should employee open the door; even though employer's improper actions took place prior to the filing of the litigation, the fruits of improper conduct had been heavily relied upon by employer in pleading and arguing the merits of its case, which accused former employee of breaching employee fiduciary duties, and infringing employer's trademarks, trade-dress, and copyrights.18 U.S.C.A. § 2701.

551 *ORDER

JOHN G. KOELTL, District Judge.

The plaintiffs' motion for a preliminary injunction is denied without prejudice to renewal.

The parties were authorized to begin expedited discovery on or after October 13, 2008. The parties should provide the Court with a Scheduling Order by October 29, 2008.

The Court has reviewed the Report and Recommendation of Magistrate Judge Katz dated August 22, 2008. No objections have been filed and the time for objections has passed. Moreover, the Court finds that the Report and Recommendation is thorough and well founded and the Court therefore adopts it. Accordingly, the Court orders that the thirty-four of defendant Alexander Fell's e-mails obtained by the plaintiffs be precluded from use in the litigation, but not for impeachment purposes should the defendants open the door. The plaintiffs are also directed to return or destroy all copies of E-mail 28, and so certify.

SO ORDERED.

Report and Recommendation

THEODORE H. KATZ, United States Magistrate Judge.

TO: HON. JOHN G. KOELTL, United States District Judge.

Plaintiffs bring this action seeking an injunction and damages, accusing Defendants of (1) stealing Plaintiffs' business model, customers, and internal documents, (2) breaching employee fiduciary duties, and (3) infringing Plaintiffs' trademarks, trade-dress, and copyrights. This case was referred to this Court for general pretrial management.

Currently before the Court is Defendants' motion to preclude the use or disclosure of thirty-four of Defendant Alexander Fell's (“Fell”) e-mails, obtained by Lauren Brenner (“Brenner”), the principal and owner of the Plaintiff corporations (“Plaintiffs”), and Fell's former employer. Defendants also seek an order requiring the e-mails' immediate return and attorneys' fees and costs.

The parties have fully briefed the issues, and, on July 18, 2008, the Court heard oral argument on the motion. Although the preclusion of evidence as a discovery sanction might normally be a non-dispositive matter for the Court to decide as part of its general pretrial supervision of a case, in this case, because of the potentially dispositive nature of the instant motion and its evidentiary implications for matters before the District Court, the District Court has requested that this Court provide a Report and Recommendation containing findings of fact, an analysis of the legal issues, and a discussion of the range of possible remedies available to the Court.

As explained in greater detail below, the Court concludes that Brenner accessed Fell's e-mails without authorization, in what would be a violation of the Stored Communications Act, 18 U.S.C. § 2707, had a cause of action been brought pursuant to that statute. The Court also concludes that, pursuant to its inherent equitable authority over the litigation process, the e-mails should be precluded, in part or in whole. Finally, the Court concludes ***552** that one e-mail is protected by the attorney-client privilege and should be returned to Defendants.

BACKGROUND

Fell was hired by Brenner in August of 2005, and worked at Pure Power Boot Camp ("PPBC"), a physical fitness center, until March 16, 2008, when Brenner fired him. On April 1, 2008, Defendant Ruben Belliard ("Belliard"), who is now Fell's business partner, and was also employed at PPBC, entered Brenner's office when she was not there, stayed there for half an hour, called Brenner on her office telephone, and quit.[FN1] A few months before he left his employ at PPBC, Belliard entered Brenner's office, again when she was not present, removed a copy of a restrictive covenant he had signed, and shredded it. (*See* Belliard Aff. ¶ 31.) Soon after Fell and Belliard left PPBC, they opened a competing fitness center, Warrior Fitness Boot Camp ("WFBC"), together with their girlfriends—Defendants Jennifer Lee ("Lee") and Nancy Baynard ("Baynard").

FN1. Brenner alleges that Belliard stole PPBC's client list and other items while he was in her office. (*See* Affidavit of Lauren Brenner, dated July 10, 2008 ("Brenner July 10 Aff."), ¶ 16.) Belliard denies he stole anything. (*See* Affidavit of Rubin Belliard, dated July 29, 2008 ("Belliard Aff."), ¶ 33.)

After Fell and Belliard were no longer working at PPBC, Brenner, on April 28, 2008, and for a week thereafter, accessed and printed e-mails from three of Fell's personal accounts: "kappamarine@ hotmail. com" ("Hotmail account"), "kappamarine@ gmail. com" ("Gmail account"), and "alex@ warrior fitness bootcamp. com" ("WFBC account"). (*See* Brenner July 10 Aff. ¶ 22; *see also* Exhibit ("Ex.") A, annexed to Declaration of Daniel Schnapp, Esq. ("Schnapp Decl."), dated July 1, 2008, E-mails 1–34; Transcript of Oral Argument, dated July 18, 2008 ("Tr."), at 14–15.) [FN2]

FN2. All references to e-mails are to the e-mails annexed to Schnapp's Declaration.

Brenner states that she was able to access Fell's Hotmail account because he left his username and password information stored on PPBC's computers, such that, when the Hotmail website was accessed, the username and password fields were automatically populated, (*See* Brenner July 10 Aff. ¶ 13.) She also alleges that Fell gave his username and password to another PPBC employee, Elizabeth Lorenzi, so that she could check on an Ebay sale he was conducting. (*See* Affidavit of Elizabeth Lorenzi, dated July 10, 2008 ("Lorenzi Aff."), ¶¶ 3, 6.) Plaintiffs allege, and Fell does not deny, that Fell accessed his Hotmail account while at work at PPBC, which is how his username and password came to be stored on the company's computers. At oral argument, Plaintiffs admitted that Brenner was able to access Fell's Gmail account because the username and password for the Gmail account were sent to Fell's Hotmail account, which Brenner accessed. (*See* Tr. at 17.) Brenner also explained that she was able to access Fell's WFBC account by making a "lucky guess" at his password, which turned out to be the same password he used for his other accounts. (*See id.* at 15–16.)

Plaintiffs have an Employee Handbook which explicitly addresses e-mail access on company computers. It states:

> "e-mail users have no right of personal privacy in any matter stored in, created on, received from, or sent through or over *the system.* This includes the use of personal e-mail accounts *on Company equipment. The Company,* in its discretion *as owner of the E–Mail system,* reserves the right to review, monitor, access, retrieve, ***553** and delete any matter stored in, created on, received from, or sent through *the system,* for any reason, without the permission of any system user, and without notice."

(Ex. A, annexed to Supplemental Affidavit of Lauren Brenner, dated June 6, 2008 ("Brenner June 6 Aff.") (emphasis added).) An additional part of the policy states: "Internet access shall not be utilized for shopping or for conducting other transactions or personal business matters." (*Id.*) Plaintiffs have not conducted a forensic evaluation of the company computers to determine what e-mails Fell actually received, sent through, read, or accessed from the company's computers. (*See* Tr. at 22,)

E-mails 1–26 and 28, were obtained from Fell's Hotmail account; of those, E-mails 1–13 and 16 are dated prior to March 16, 2008, the date Fell stopped working at PPBC, E-mails 27, 29–31, 33, and 34 were obtained from Fell's Gmail account. E-mail 32 was obtained from Fell's e-mail account at WFBC.

Fell states in his affidavit that all of the e-mails were drafted or received on his own home computer. (*See* Affidavit of Alex Fell, dated July 1, 2008 ("Fell Aff."), ¶ 5.) Fell denies that he ever gave his Hotmail information to anyone at PPBC. (*See id.* ¶ 4.) Fell does not deny, however, that he may have viewed some of his e-mails on PPBC's computers while he was working there.

While it is not possible to determine from the submissions when the e-mails were read, they do indicate the date and time they were sent. E-mails sent by Fell indicate that they were sent at all times during the day, on various days of the week. For example, E-mail 4 shows that Fell sent a message on Monday, February 11, 2008 at 3:09 p.m. in the afternoon. E-mail 6 was sent on Wednesday, February 20, 2008 at 2:37 p.m. On Thursday, February 28, 2008, Fell sent E-mail 9 at 3:35 in the morning. E-mail 16 was sent the day before Fell was fired, Saturday, March 15, 2008 at 5:06 p.m. Each of these e-mails relates to, or discusses his efforts to set up his competing business—WFBC.[FN3]

> FN3. Fell makes a general claim that he never did any work related to WFBC while he was at PPBC or on PPBC computers. (*See* Fell Aff. ¶ 6.) However, he has not provided his PPBC work schedule, so there is no way to confirm whether or not he was at PPBC when he sent any of these e-mails.

Plaintiffs have relied heavily upon the e-mails and have considered them critical to their case. The e-mails provide a detailed picture of Fell's and Belliard's efforts to set up WFBC before they left PPBC, the work that Lee and Baynard did to support those efforts—including recruiting PPBC clients for WFBC while they themselves were still clients of PPBC, and the fallout after Fell and Belliard left PPBC. For example, E-mail 29 is a candid admission that Belliard shredded his non-compete contract with PPBC, a fact Defendants attempted to avoid revealing during prior state court proceedings. (*See* Ex. B annexed to Declaration of Daniel Schnapp, dated July 3, 2008, transcript of proceedings before Hon. Helen Freedman, New York Supreme Court, dated May 8, 2008 ("NY Tr."), at 28.) E-mail 21 shows a dramatic expansion of WFBC's customer list, and includes a large number of former PPBC clients and their e-mail addresses, which Plaintiffs rely upon to show that Belliard stole PPBC's client list. (*See* Declaration of Richard Herzfeld, Esq., dated July 11, 2008, ¶ 25.)

Some of the e-mails were sent to, or received

from, Defendants' attorneys. (*See* E-mails 12, 13, 14, 28.) [FN4] E-mail 13 ***554** was sent from a legal assistant at Fox Rothschild, Defendants' counsel, attaching an IRS document containing WFBC's employer ID number. E-mail 14, from the same paralegal, attached WFBC's Articles of Organization, and informed Fell that they were filed with the State of New York. E-mail 28 is from an attorney at Fox Rothschild, and appears to have been printed from Fell's "sent" file; it is part of an e-mail chain consisting of back-and-forth e-mails from the same Fox Rothschild attorney, and contains advice about how to handle telephone calls from Brenner.

> FN4. Defendants did not include "E-mail 12" in their submissions, although it is described and referred to in the pleadings. (*See* Defendants' Memorandum of Law in Support of Their Motion for an Order Precluding the Use or Disclosure of Specific Emails ("Defs.' Mem."), at 7.) According to Defendants, E-mail 12 is a privileged e-mail from Defendants' attorneys. (*See id.*)

When Plaintiffs first filed suit seeking a temporary restraining order and preliminary injunction in state court, they used the challenged e-mails as exhibits. However, at the time the e-mails were provided to Defendants, the bottom part of the page, which shows when an e-mail was printed, was obscured or removed. (*See* all e-mails in Ex. A.) Defendants allege that this amounts to spoliation of evidence. In response, during oral argument, Plaintiffs stated that they had the original copies of the e-mails, showing when they were printed, and agreed to provide unredacted copies to Defendants. (*See* Tr. at 33–34.)

DISCUSSION

Defendants seek the preclusion and return of Fell's e-mails, claiming that Brenner violated the Electronic Communications Privacy Act, 18 U.S.C. § 2510 ("ECPA"), the Stored Communications Act, 18 U.S.C. § 2707 ("SCA"), and New York Penal Law § 250.05, when she accessed Fell's e-mail accounts. Defendants also argue that some e-mails are protected by attorney-client privilege. Finally, Defendants argue that Plaintiffs' production of the e-mails with the dates on which they were printed obscured, amounts to spoliation of evidence, further justifying preclusion.

Plaintiffs argue that the ECPA and New York Penal Law do not apply, and that, in any event, Fell gave implied consent which authorized Brenner's access. Plaintiffs also argue that the crime-fraud exception to confidentiality should apply not only to any e-mails covered by the attorney-client privilege, but to all the e-mails accessed by Brenner. Finally, Plaintiffs argue that the redaction of the printing dates does not constitute sanctionable spoliation.

It is important to note from the outset, that this is not a situation in which an employer is attempting to use e-mails obtained from the employer's own computers or systems. Rather, the e-mails at issue here were stored and accessed directly from accounts maintained by outside electronic communication service providers. Furthermore, Defendants have not directly asserted any claims under the statutes they allege Brenner violated, and instead, appeal only to the Court's inherent equitable authority to preclude evidence wrongfully obtained, outside of the litigation process, from being used in the litigation. Thus, while Defendants invoke federal and state law, those laws are invoked solely for the Court to consider as part of the process of weighing the competing equitable considerations raised by the conduct of both sides to this dispute.

I. *The Statutes*

All three of the statutes Defendants rely upon are criminal statutes that also provide relief to aggrieved parties in civil causes of action. Of the three statutes, however, only the Stored Communications Act is applicable.

***555** A. *The Stored Communications Act*

[1] The Stored Communications Act, 18 U.S.C. § 2701, et seq. ("SCA"), part of the Wiretap Act, provides in part:

> (a) Offense.—Except as provided in subsection (c) of this section whoever—
>
> (1) intentionally *accesses without authorization a facility through which an electronic communication service is provided;* or
>
> (2) intentionally *exceeds an authorization* to access that facility; and *thereby obtains*, alters, or prevents authorized access to a wire or *electronic communication while it is in electronic storage* in such system shall be punished as provided in subsection (b) of this section.

18 U.S.C.A. § 2701 (emphasis added). The Act "aims to prevent hackers from obtaining, altering or destroying certain stored electronic communications." *In re DoubleClick Inc. Privacy Litigation*, 154 F.Supp.2d 497, 507 (S.D.N.Y.2001) (citing *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F.Supp.2d 817, 820 (E.D.Mich.2000)). Thus, a person violates the SCA if she accesses an electronic communication service, *or* obtains an electronic communication while it is still in electronic storage, without authorization.

"Electronic storage," defined in an earlier part of the Wiretap Act is: "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication ...." 18 U.S.C. §§ 2510(17), 2711(1) (definitions of Wiretap Act applicable to Stored Communications Act).

The majority of courts which have addressed the issue have determined that e-mail stored on an electronic communication service provider's systems after it has been delivered, as opposed to e-mail stored on a personal computer, is a stored communication subject to the SCA. *See United States v. Councilman*, 418 F.3d 67, 79 (1st Cir.2005) (en banc) (describing in detail the nature of e-mail, and concluding that "the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process for such communications."); *see also Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 115 (3rd Cir.2003) (holding that e-mail stored on the defendant's system was subject to the SCA); *cf. Hall v. EarthLink Network, Inc.*, 396 F.3d 500, 503 n. 1 (2d Cir.2005) (finding unpersuasive the argument that an e-mail in storage is not an "electronic communication").

In a case analogous to this one, *Bailey v. Bailey*, No. 07 Civ. 11672, 2008 WL 324156 (E.D.Mich. Feb. 6, 2008), the ex-husband defendant installed a keystroke logger on a computer shared by him and his then-wife, which allowed him to learn her password to her Yahoo account (among others), and which he used to access her e-mail directly from her Yahoo account. *See id.* at *3. The wife filed suit pursuant to the SCA, as well as under 18 U.S.C. § 2511, the ECPA. *See id.* The court denied a motion for summary judgment brought by the defendant, who claimed that neither statute applied, and determined that e-mails, "received by the intended recipient where they remain stored by an electronic communication service," are covered by the SCA. *Id.* at *6 (citing *Theofel v. Farey–Jones*, 359 F.3d 1066 (9th Cir.2003)).

In this case, Brenner obtained Fell's username and password to his Hotmail account because he left that information stored on Plaintiffs' computers. She then used that information to go into his Hotmail account, and read and printed his e-mails. Some of those e-mails may have been read by Fell while he was at work, but there is no evidence indicating which ***556** e-mails he may have viewed on Plaintiffs' computers,

and there is no evidence that the e-mails were downloaded onto PPBC's computers. At most, only e-mails dated prior to his last day of work could have been viewed by him and thus potentially stored on the company's systems.

In any event, Brenner did not use an examination of PPBC's computer's memory to determine what Fell accessed at work. Instead, she logged directly onto Microsoft's Hotmail system where the e-mails were stored, and viewed and printed them directly off of Hotmail's system. She accessed Fell's other accounts in the same manner, and there is no evidence indicating that Fell accessed his Gmail or WFBC accounts at any time while he worked at PPBC. By Plaintiffs' own admission, Brenner obtained the username and password for the Gmail account from Fell's Hotmail account, and made a "lucky guess" that Fell would use the same password for all three accounts, including his WFBC account.

Thus, Brenner accessed three separate electronic communication services, and she obtained Fell's e-mails while they were in storage on those service providers' systems. Either of those actions, if done without authorization, would be a violation of the SCA. *See Wyatt Technology Corp. v. Smithson,* No. CV 05–1309(DT), 2006 WL 5668246, *9 (C.D.Cal. Aug.14, 2006) (granting summary judgment in favor of counter-claimant alleging that the plaintiff violated the SCA by accessing the defendant's personal e-mail on a private foreign server, and monitoring the personal e-mail account, without authorization).

B. *The Electronic Communications Privacy Act*

[2] The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2511 ("ECPA"), creates criminal sanctions and a civil cause of action against persons who "intercept" electronic communications.[FN5] In the context of unauthorized access to e-mail, the question that courts have struggled with is determining whether one can "intercept" an e-mail that has already been delivered. The Second Circuit has not directly addressed this question, but has discussed the issue in at least one case. *See Hall,* 396 F.3d at 503 n. 1.

FN5. 18 U.S.C.A. § 2515 reads;

> Whenever any *wire or oral communication* has been *intercepted,* no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

In *Hall,* the Second Circuit held that the ECPA was applicable to the e-mails at issue because "the case involve[d] the *continued receipt* of e-mail messages rather than the acquisition of *previously stored* electronic communication." 396 F.3d at 503 n. 1 (emphasis in original). The Circuit was unpersuaded by the defendant's argument that "an 'interception' [as required by the ECPA,] can only occur when messages are in transit," but did not elaborate further. *Id.* Rather, it factually distinguished the cases cited by the defendant—which held that e-mails no longer in transit cannot be "intercepted." *See id.* (distinguishing: *Fraser,* 352 F.3d at 110; *United States v. Steiger,* 318 F.3d 1039, 1048–49 (11th Cir.2003); *Konop v. Hawaiian Airlines, Inc.,* 302 F.3d 868, 873, 876–79 (9th Cir.2002); *Steve Jackson Games, Inc. v. United States Secret Serv.,* 36 F.3d 457, 460–64 (5th Cir.1994)).

Hall is itself factually distinguishable from this case. *Hall* involved the continued ***557** and contemporaneous acquisition of e-mails as part of the ordinary course of the defendant's business—which was the internet communication service provider for the e-mails in question. *See id.* Here, PPBC is not an

internet communications provider, and Brenner did not access the e-mails on a continuous basis, contemporaneous with their transmission. Rather, by the time Brenner viewed the e-mails, they had been delivered to Fell's accounts, and may have already been viewed by him; thus, they were "previously stored electronic communications"—precisely the situation which *Hall* relied upon to distinguish the decisions the defendants relied upon in that case. *See id.*

Other courts which have considered the question of whether accessing an electronic communication that has already been delivered is "intercepted," have found that the ECPA does not apply. *See Fraser*, 352 F.3d at 113–14 (holding that the defendant did not "intercept" the plaintiff's e-mail by accessing e-mail stored on its central file server, because "an 'intercept' under the ECPA must occur contemporaneously with transmission"); *Steiger*, 318 F.3d at 1048–49 (declining to suppress evidence obtained by a hacker from defendant's computer, pursuant to the ECPA, because "a contemporaneous interception—*i.e.*, an acquisition during "flight"—is required to implicate the [ECPA] with respect to electronic communications"); *Konop*, 302 F.3d at 873, 878–80 (noting subsequent changes in the Wiretap Act support the conclusion that accessing a secure website did not constitute an "interception" of an electronic communication under the ECPA, and narrowly defined interception as "contemporaneous interception").

As the court in *Bailey* explained: "The general reasoning behind these decisions is that based on the statutory definition and distinction between 'wire communication' and 'electronic communication,' the latter of which conspicuously does not include electronic storage, Congress intended for electronic communications in storage to be handled solely by the Stored Communications Act." *Bailey*, 2008 WL 324156, at *4; *see also Fraser*, 352 F.3d at 113–14 (explaining the statutory interpretation issues). Thus, in those cases which have examined whether the ECPA or the SCA should apply to delivered e-mails, courts have concluded that the SCA, not the ECPA, is the proper statute to apply in situations similar to this case. *See Steiger*, 318 F.3d at 1049 (noting that "the SCA may apply [in this case] to the extent the source accessed and retrieved any information stored with Steiger's Internet service provider").

Defendants concede that the ECPA has a requirement of contemporaneous interception. (*See* Tr. at 12.) Nonetheless, Defendants suggest that Brenner's access to Fell's e-mail was "contemporaneous" if it occurred during some undefined, short period of time after the e-mail had been delivered. (*See* Tr. at 12–13.) However, they have not provided any authority for that proposition, nor have they suggested how long a "contemporaneous time frame" would be. (*Id.*) In any event, there is no evidence of when Brenner accessed Fell's e-mails, but its clear that the majority of the e-mails were sent or received prior to April 28, 2008, the earliest date that Brenner admits that she accessed and printed them. Additionally, there is no evidence that the later e-mails were intercepted at the same time that they were delivered. Rather, the evidence indicates that Brenner periodically accessed Fell's e-mail accounts and printed e-mails after they had been delivered.

Applying the definition of "intercept" accepted by the majority of courts to have examined the issue, the Court concludes that Brenner did not access and print ***558** Fell's e-mails contemporaneous with their transmission. *See Fraser*, 352 F.3d at 113–14. Therefore, the Court concludes that Brenner did not violate the ECPA.

C. *New York Eavesdropping and Civil Procedure Laws*

Defendants argue that Brenner also violated New York's eavesdropping law, and, pursuant to a New York procedural rule, Fell's e-mails should be precluded. New York Penal Law § 250.05 makes it a crime for a person to "unlawfully engage in wiretapping, ... or intercepting or accessing [an] electronic commu-

nication." N.Y. Penal Law § 250.05 (McKinney 2008). New York Civil Practice Law and Rule § 4506 ("CPLR § 4506") states:

> "The contents of any overheard or recorded communication, conversation or discussion, or evidence derived therefrom, which has been obtained by conduct constituting the crime of eavesdropping, as defined by section 250.05 of the penal law, may not be received in evidence in any trial, hearing or proceeding before any court ...."
>
> N.Y. C.P.L.R. § 4506 (Consol.2008).

[3] If a party to a civil action seeks preclusion pursuant to § 4506, it must bring a motion "before a justice of the supreme court ...." *Id.* at § 4506(4). In contrast to the federal laws, New York's rule does not provide a separate civil cause of action, but, rather, is only a vehicle through which evidence may be excluded in an underlying case. *See id.* It also does not provide for damages, attorneys' fees, costs, or any remedy other than exclusion of the evidence. *See id.*

There is a notable dearth of state law construing CPLR § 4506. Defendants have not cited, and the Court has not found, any published cases applying CPLR § 4506 to unauthorized access to e-mail. On its face, however, the statute does not appear to apply in this situation. The plain language of the statute seems to limit its application to the contents of an "overheard or recorded communication." CPLR § 4506. Furthermore an aggrieved person is defined as one whose "communication, conversation or discussion was unlawfully *overheard or recorded.*" *Id.* at § 4506(3)(a). In addition, the statute only makes reference to "telephonic or telegraphic communication[s]," not electronic communications. *Id.* at § 4506(2)(a). This language seems to limit the application of the statute to communications obtained aurally, rather than to electronic communications such as e-mail.[FN6]

> FN6. The Court also notes that Penal Law § 250.05 explicitly includes "electronic communications" while CPLR § 4506 does not, suggesting that e-mails obtained in violation of Penal Law § 250.05 are not subject to exclusion under CPLR § 4506.

Furthermore, neither party has briefed the fundamental and more complex issue of whether CPLR § 4506, a rule governing the exclusion of evidence in New York state courts, ought to be applied by this Court pursuant to *Erie R. Co. v. Tompkins*, 304 U.S. 64, 58 S.Ct. 817, 82 L.Ed. 1188 (1938).[FN7] *Cf. United States v. Canniff*, 521 F.2d 565, 568 (2d Cir.1975) ("Under New York law (which, however, is not controlling in this federal proceeding), [evidence] of a youthful offender adjudication for the purpose of impeachment is prohibited ...." (internal citation omitted)).

> FN7. There are both federal and state law substantive claims in this action.

Ultimately, a determination of the meaning of CPLR § 4506 is unnecessary, and better left to the New York state courts. The Court could preclude use of the e-mails pursuant to the SCA or its inherent authority, without applying CPLR § 4506. Thus, there is no need to resolve the issues ***559** of whether CPLR § 4506 is applicable to this action and, if so, whether it mandates the preclusion of the e-mails.

D. *Authorization*

Accessing and obtaining e-mails directly from an electronic communication service provider is a violation of the SCA if done without authorization. Having determined that the SCA is applicable to Brenner's conduct, she therefore may not have violated the SCA if she was authorized to access Fell's e-mail accounts.

Plaintiffs argue that Brenner was authorized to view and print Fell's e-mails, and assert two theories in

support of this position. First, Plaintiffs claim that PPBC's e-mail policy put Fell on notice that his e-mails could be viewed by Brenner, and thus he had no expectation of privacy in his Hotmail account. Second, Plaintiffs argue that even if he had an expectation of privacy, Fell, by leaving his username and password on PPBC's computers, gave Brenner implied consent to access his accounts.

Defendants respond by denying that Fell gave PPBC, or any of its agents or employees, authorization to access his accounts, and specifically deny that Fell gave his username and password to Brenner's assistant. Defendants also deny that PPBC had its e-mail policy in place during Fell's employment, and suggest that it is a recent creation by Brenner. (*See* Tr. at 4–5.) In any event, they argue that it does not cover e-mails sent after Fell left PPBC's employ.

Brenner claims Fell had no expectation of privacy in his e-mails and that Fell gave implied consent to unlimited access to all of Fell's personal e-mail accounts, with no time constraints (not even for the period after Fell's employment at PPBC ended), based on her assertion that Fell accessed his personal Hotmail account, at least once, on Plaintiffs' computer. These arguments have no sound basis in fact, law, or logic.

As an initial matter, Plaintiffs' position is not supported by PPBC's policy. PPBC's e-mail policy—the basis of Plaintiffs' consent defense—is, by its own terms, limited to "Company equipment." The reservation of rights is explicitly limited to "any matter stored in, created on, received from, or sent through [PPBC's] system." [FN8] Therefore, it could not apply to e-mails on systems maintained by outside entities such as Microsoft or Google. In addition, there is no evidence that the e-mails in issue were created on, sent through, or received from PPBC's computers. Moreover, Plaintiffs' position makes no distinction between the Hotmail account Fell accessed while at work, and the other accounts, which by all appearances were never accessed by Fell at work, and may not even have existed until after he left PPBC's employ.

> FN8. Even the case Plaintiffs rely upon, in support of the argument that Fell waived his right to privacy in his Hotmail account, acknowledges that an employer's e-mail policy is limited only to e-mails viewed by employees while at work. *See Scott v. Beth Israel Med. Ctr. Inc.*, 17 Misc.3d 934, 938, 847 N.Y.S.2d 436, 440 (N.Y.Sup.2007) (noting that "the effect of an employer e-mail policy ... is to have the employer looking over your shoulder each time you send an e-mail").

Plaintiffs' position-that Brenner was authorized to access Fell's e-mails on his personal e-mail service providers' systems through his implied consent—also has no support in the law. To understand the basis of Plaintiffs' argument, and why it has no legal support, it is important to first understand the framework within which the typical employee e-mail case usually arises. Courts have routinely found that employees have no reasonable expectation of privacy in their workplace computers, ***560** where the employer has a policy which clearly informs employees that company computers cannot be used for personal e-mail activity, and that they will be monitored. *See United States v. Simons*, 206 F.3d 392, 398 (4th Cir.2000) ("Therefore, regardless of whether Simons subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after FBIS notified him that it would be overseeing his Internet use."); *Thygeson v. U.S. Bancorp*, No. CV–03–467–ST, 2004 WL 2066746, *21 (D.Or. Sept.15, 2004) ("when, as here, an employer accesses its own computer network and has an explicit policy banning personal use of office computers and permitting monitoring, an employee has no reasonable expectation of privacy."); *Muick v. Glenayre Electronics*, 280 F.3d 741, 743 (7th Cir.2002) ("But Glenayre

had announced that it could inspect the laptops that it furnished for the use of its employees, and this destroyed any reasonable expectation of privacy that Muick might have had and so scotches his claim."). In these cases, because the employee had no reasonable expectation of privacy, the employer did not need consent to search the employee's computer files.

[4] This is not, however, a case where an employee was using an employer's computer or e-mail system, and then claimed that the e-mails contained on the employer's computers are private. Here, the employee—Fell—did not store any of the communications which his former employer now seeks to use against him on the employer's computers, servers, or systems; nor were they sent from or received on the company e-mail system or computer. These e-mails were located on, and accessed from, third-party communication service provider systems. There is not even an implication that Fell's personal e-mail accounts were used for PPBC work, or that PPBC paid or supported Fell's maintenance of those accounts. *See, e.g., Rozell v. Ross–Hoist,* No. 05 Civ. 2936(JGK)(JCF), 2006 WL 163143, *2–3 (S.D.N.Y. Jan. 20, 2006) (ordering production of e-mails taken from a personal third-party communication service provider account, which served as a back-up for work related communications). Furthermore, there is nothing in the PPBC policy that even suggests that if an employee simply views a single, personal e-mail from a third party e-mail provider, over PPBC computers, then all of the his personal e-mails on whatever personal e-mail accounts he uses, would be subject to inspection. In short, this case is distinguishable from those cases which hold that employees have no expectation of privacy in e-mails sent from or received and stored on the employer's computers.

Even in cases involving an employer's search of an employee's work computer, courts have held that, under certain circumstances, employees have a reasonable expectation of privacy in the contents of their work computer. For example, in *Leventhal v. Knapek,* 266 F.3d 64, 74 (2d Cir.2001), the Second Circuit held that an employee had a reasonable expectation of privacy in the contents of his computer where the employee occupied a private office with a door, had exclusive use of the computer in his office, and did not share use of his computer with other employees or the public, notwithstanding the fact that there was a policy which "prohibited 'using' state equipment 'for personal business.' " In *Leventhal,* there was no clear policy or practice regarding regular monitoring of work computers; technical staff conducted infrequent and selective searches for maintenance purposes only. *See id.*

In *Curto v. Medical World Communications,* No. 03 Civ. 6327 (DRH) (MLO), 2006 WL 1318387 (E.D.N.Y. May 15, 2006), the employer hired a forensic consultant***561** to restore portions of the computer files that the employee had deleted, nearly two years earlier, from a home-based work computer, including e-mails of communications with the employee's lawyer. *See id.* at *1. Even though the computer belonged to the employer, and the employer had a policy that warned employees they had no reasonable expectation of privacy in "anything they create, store, send, or received on the computer, or through the Internet or any computer network," the employee successfully asserted attorney-client privilege over those e-mails, in part because she had a reasonable expectation of privacy in a home-computer which was not connected to the employer's network. *See id.* at *8.

And, in a recent case from the Ninth Circuit Court of Appeals, in which violations of both the SCA and the Fourth Amendment were alleged, that court held that a police officer had a reasonable expectation of privacy in text messages sent using a city-owned pager. *See Quon v. Arch Wireless,* 529 F.3d 892, 908 (9th Cir.2008) (concluding that "a reasonable juror could conclude ... that plaintiff expected that his call to his wife would be private, and that expectation was objectively reasonable").

Here, Fell had a subjective belief that his personal e-mail accounts, stored on third-party computer systems, protected (albeit ineffectively) by passwords, would be private. That expectation of privacy was also reasonable, as nothing in PPBC's policy suggests that it could extend beyond Plaintiffs' own systems, and beyond the employment relationship. Furthermore, there is no evidence that PPBC's policy was clearly communicated to its employees, or that it was consistently enforced in a manner that would have alerted employees to the possibility that their private e-mail accounts, such as Hotmail, could also be accessed and viewed by their employer.

Because Fell had a reasonable expectation of privacy in his e-mail accounts, Brenner could only be authorized to access those accounts if Fell had given consent. She argues that Fell gave her implied consent to search his e-mails because he left his login information stored on PPBC's computers where it could be discovered and used by Brenner. The Court does not accept Plaintiffs' argument.

There is no sound basis to argue that Fell, by inadvertently leaving his Hotmail password accessible, was thereby authorizing access to all of his Hotmail e-mails, no less the e-mails in his two other accounts. If he had left a key to his house on the front desk at PPBC, one could not reasonably argue that he was giving consent to whoever found the key, to use it to enter his house and rummage through his belongings. And, to take the analogy a step further, had the person rummaging through the belongings in Fell's house found the key to Fell's country house, could that be taken as authorization to search his country house. We think not. The Court rejects the notion that carelessness equals consent. *See Lipin v. Bender*, 193 A.D.2d 424, 426, 597 N.Y.S.2d 340, 341 (1st Dep't 1993) (rejecting the argument that because documents "had been left unsecured, directly in front of the plaintiff, in a public area, ... plaintiff had been 'invited' to read the documents").

Implied consent, at a minimum, requires clear notice that one's conduct may result in a search being conducted of areas which the person has been warned are subject to search. *Cf. United States v. Workman*, 80 F.3d 688, 694 (2d Cir.1996) (holding that a posted sign and an inmate handbook, providing notice that telephone calls would be monitored, together with inmate's "plain awareness that his conversations were subject to monitoring," amounted to implied consent to surveillance); ***562***United States v. Amen*, 831 F.2d 373, 378–79 (2d Cir.1987) (prisoners gave implied consent to interception of telephone calls because they were on notice from at least four sources, including actual direct notice); *Sec. and Law Enforcement Employees v. Carey*, 737 F.2d 187, 202 n. 23 (2d Cir.1984) (noting that an important consideration in determining whether a person has consented to being searched is "evidence that the person had knowledge of the right to refuse to give consent;" and rejecting the argument that correction officers consented to being strip-searched "merely by accepting employment and by receiving [a] rule book [giving notice that the Department's employees, while on correctional facility property, were subject to being searched]"); *Anobile v. Pelligrino*, 303 F.3d 107, 124–25 (2d Cir.2002) (rejecting an assertion that racetrack employees, by signing a license with a "a blanket waiver of the right to object to any future searches," gave an effective consent to search their dormitory rooms, because "there [was] no evidence demonstrating that the plaintiffs were aware of their right to refuse to give consent to this unconstitutional search or indeed whether they could refuse and still obtain employment").

In this case, Fell only had notice that PPBC's computers could be searched for evidence of personal e-mail use, not that his Hotmail, Gmail, or WFBC e-mail accounts would also be searched. He was also never given the opportunity to refuse Brenner any authorization to search his e-mails. At most, one could argue that Fell have consented to Brenner viewing his password. But he did not consent to her to using it.

Absent clear knowledge of the extent of what could be searched, and the opportunity to refuse or withdraw his consent, the Court rejects Plaintiffs' argument that Fell gave implied consent to Brenner to search his Hotmail account simply by leaving his password on her computer.

Even less sustainable is the proposition that correctly "guessing" a person's password, as Brenner did, amounts to authorization to access all accounts which use that password. Were that the case, computer hackers across the country could escape liability for breaking into computer systems by correctly "guessing" the codes and passwords of their victims. This absurd result stands in direct conflict with the entire purpose of the SCA and basic principles of privacy. *See In re DoubleClick*, 154 F.Supp.2d at 507.

The Court is convinced that Fell accessed his Hotmail account at some point when he was working at PPBC, and left his username and password stored on PPBC's computer. Otherwise, Brenner could not have obtained Fell's password, thereby making it possible for her to access his Hotmail account.[FN9] Nonetheless, the Court concludes that Brenner's access to Fell's Hotmail account violated the SCA and Fell's privacy. While Fell arguably "authorized" access to any e-mails which he viewed and saved on PPBC's computers, Brenner was not authorized to access those e-mails directly from Fell's Hotmail account, and was clearly not authorized to access e-mails from Fell's Gmail and WFBC accounts.

> FN9. Defendants' suggestion that Brenner used a keystroke logging program is rank speculation, and, even if it were true, would only confirm that Fell entered his Hotmail password into PPBC's computers to access his Hotmail account.

II. *Privilege and the Crime–Fraud Exception*

Independent of whether the e-mails should be precluded because they were improperly secured, Defendants also assert that certain of these e-mails should be precluded, and they should be returned, ***563** because they are subject to the attorney-client privilege.

Plaintiffs' respond that the e-mails in question are not privileged communications. Plaintiffs also argue that Fell forfeited any right of privacy to all of his e-mails because those e-mails were in furtherance of what Plaintiffs describe as "civil and criminal misconduct." (Plaintiffs' Memorandum of Law in Opposition to the Motion to Preclude Use of E-mails ("Pls.' Mem."), at 9.) Thus, Plaintiffs invoke the crime-fraud exception to confidentiality, normally applicable to attorney-client privilege claims, and assert that Fell forfeited his right to privacy in *all* of his e-mails, including, but not limited to, e-mails covered by the attorney-client privilege.

[5][6][7] The attorney-client privilege affords confidentiality to communications among clients and their attorneys, for the purpose of seeking and rendering an opinion on law or legal services, or assistance in some legal proceeding, so long as the communications were intended to be, and were in fact, kept confidential. *See United States v. Int'l Bhd. of Teamsters*, 119 F.3d 210, 214 (2d Cir.1997); *United States v. Doe (In re Six Grand Jury Witnesses)*, 979 F.2d 939, 943 (2d Cir.1992); *John Doe Corp. v. United States (In re John Doe Corp.)*, 675 F.2d 482, 487–88 (2d Cir.1982); *Bank Brussels Lambert v. Credit Lyonnais (Suisse) S.A.*, 160 F.R.D. 437, 441 (S.D.N.Y.1995) (citing *United States v. United Shoe Mach. Corp.*, 89 F.Supp. 357, 358–59 (D.Mass.1950)). The privilege is among the oldest of the common law privileges and "exists for the purpose of encouraging full and truthful communication between an attorney and his client." *In re von Bulow*, 828 F.2d 94, 100 (2d Cir.1987); *accord United States v. Bilzerian*, 926 F.2d 1285, 1292 (2d Cir.1991). However, because the privilege "stands as an obstacle of sorts to the search for truth," it must be applied "only

to the extent necessary to achieve its underlying goals." *XYZ Corp. v. United States (In re Keeper of the Records),* 348 F.3d 16, 22 (1st Cir.2003); *see also Salomon Bros. Treasury Litig. v. Steinhardt Partners (In re Steinhardt Partners),* 9 F.3d 230, 235 (2d Cir.1993) (finding that the privilege does not apply in situations where the client's conduct does not serve to "improve [ ] the attorney-client relationship") (quoting *Permian Corp. v. United States,* 665 F.2d 1214, 1221 (D.C.Cir.1981)). Thus, in order to merit protection, the "predominant purpose" of the communication must be to render or solicit legal advice, as opposed to business or policy advice. *See In re County of Erie,* 473 F.3d 413, 420 (2d Cir.2007). Finally, "the burden of establishing the existence of an attorney-client privilege, in all of its elements, rests with the party asserting it." *United States v. Doe (In re Grand Jury Proceedings),* 219 F.3d 175, 182 (2d Cir.2000) (quoting *Int'l Bhd. of Teamsters,* 119 F.3d at 214).

[8][9] The attorney-client privilege is waived if the holder of the privilege voluntarily discloses or consents to disclosure of any significant part of the communication to a third party or stranger to the attorney-client relationship. *See In re Grand Jury Proceedings,* No. M–11–189 (LAP), 2001 WL 1167497, at *7 (S.D.N.Y. Oct.3, 2001); *In re Kidder Peabody Sec. Litig.,* 168 F.R.D. 459, 468 (S.D.N.Y.1996). Finally, a party who seeks to uphold the privilege must take affirmative measures to maintain the confidentiality of attorney-client communications. *See In re Steinhardt Partners,* 9 F.3d at 235; *In re von Bulow,* 828 F.2d at 100; *In re Horowitz,* 482 F.2d 72, 82 (2d Cir.1973).

A. *E-mails Protected by Attorney–Client Privilege*

Defendant claims that E-mails 12, 13, 14, and 28 are protected by the attorney-client ***564** privilege. E-mail 12, though referred to by the parties, was not provided with Defendants' motion papers. Defendants' counsel represents that it is an e-mail sent to Fell by a legal assistant at Fox Rothschild, the law firm representing Defendants. E-mail 13 was sent to Fell from a paralegal at Fox Rothschild, merely transmitting WFBC's employer ID number; attached is correspondence from the IRS. E-mail 14, from the same paralegal, indicates that WFBC's Articles of Organization were filed with the State of New York, and the Articles are attached. E-mail 28 is from an attorney at Fox Rothschild, and appears to be printed from Fell's "sent" file because the first part of the e-mail is a message from Fell to the attorney, as the end of a chain of back-and-forth e-mails from the same attorney. The e-mail contains advice about how to handle telephone calls from Brenner.

[10] E-mails 13 and 14, sent to Fell from a paralegal at Fox Rothschild, are not communications seeking or rendering an opinion on law or legal services, and the information they contain is business information that is a matter of public record. The fact that the e-mails contain a warning indicating they contain "PRIVILEGED AND CONFIDENTIAL INFORMATION," does not transform them from non-privileged communications into privileged communications. *See In re Grand Jury Proceedings,* 2001 WL 1167497, at *10 ("[T]he determination of whether a document is privileged does not depend upon ... a privilege legend."). The Court therefore concludes that E-mails 13 and 14 are not privileged.

Defendants have not met their burden of demonstrating that E-mail 12 should be protected by the attorney-client privilege. This e-mail has not been provided to the Court for review, and the description provided in Defendants' memorandum of law is far too vague, and simply makes the conclusory assertion that it is subject to attorney-client privilege. Accordingly, the Court concludes that E-mail 12 is not privileged. *See* Fed.R.Civ.P. 26(b)(5)(A)(ii) ("the party must ... describe the nature of the documents, communications, ... and do so in a manner that ... will enable other parties to assess the claim").

E-mail 28 is different. That e-mail is actually a series of communications, sent a month after Fell left

PPBC, in which Fell, using his Hotmail account, sought advice from a Fox Rothschild attorney about how to handle telephone calls from Brenner. The attorney responds by providing advice and seeking additional information. Fell then responds with the additional information, and the attorney again provides specific legal advice. The communication ends with Fell thanking the attorney for the advice.

The Court concludes that this e-mail is protected by attorney-client privilege. It was clearly conveying information and legal advice, as well as the attorney's thoughts and impressions about the strengths of Fell's, and the other Defendants', legal position. There is some question, however, about the measures Fell took to keep the communications confidential, and whether it was objectively reasonable for him to expect that his communications would be kept private.

[11] On the one hand, according to his affidavit, Fell was using his own personal home computer to communicate with his attorney on a private e-mail account. It is generally accepted that lawyers and clients may communicate confidential information through unencrypted e-mail and reasonably maintain an expectation that the communications are private and confidential. *See In re Asia Global Crossing*, 322 B.R. at 256 (citing N.Y. C.P.L.R. § 4548 (McKinney 1999), stating that a privileged communication does not lose its privilege ***565** for the sole reason it was sent by e-mail); *cf. In re County of Erie*, 473 F.3d at 422 (finding e-mails between county attorney and sheriff's office, sent with the predominant purpose of legal advice, were privileged so long as they were not shared with others); *Geer v. Gilman Corp.*, No. 06 Civ. 889(JBA), 2007 WL 1423752, *4 (D.Conn. Feb.12, 2007) ("[P]laintiff's attorney-client privilege in communications with her counsel was not waived by virtue of her having used her fiance's computer and e-mail address ... [because] plaintiff took affirmative steps to maintain the confidentiality of the attorney-client communications.").

On the other hand, Fell left his Hotmail account vulnerable to the prying eyes of other parties by leaving his password stored on PPBC's computer, and possibly by giving his login and password information to a PPBC employee.

Nonetheless, the Court has already concluded above that Fell had a reasonable subjective and objective belief that his communications would be kept confidential—and this includes his communications with his attorney. Even if Fell was fully aware of Plaintiffs' policy concerning e-mail, there is nothing in that policy that would have alerted him that, after he left Plaintiffs' employ, Brenner might search his personal e-mails sent though his personal computer, and stored on his personal internet providers' systems. Although Fell ultimately failed to properly protect his Hotmail password, there is no evidence that leaving it on PPBC's computers was anything but inadvertent. Thus, it remained reasonable for him to expect that the contents of his personal e-mails, particularly those written and sent after his employment at PPBC had ended, would be kept private when he sought the advice of his attorney. *See In re County of Erie*, 473 F.3d at 422; *Geer v. Gilman Corp.*, 2007 WL 1423752, at *4.

However, finding E-mail 28 is protected by the attorney-client privilege does not end the inquiry. Plaintiffs also argue that the privilege should be overcome based on the crime-fraud exception.

B. *The Crime–Fraud Exception*

The protections of the attorney-client privilege may be lost if the crime-fraud exception applies. "[T]he purpose of the crime-fraud exception to the attorney-client privilege [is] to assure that the 'seal of secrecy,' between lawyer and client does not extend to communications 'made for the purpose of getting advice for the commission of a fraud' or crime." *United States v. Zolin*, 491 U.S. 554, 562–563, 109 S.Ct. 2619, 2626, 105 L.Ed.2d 469 (1989); *see also In re John Doe, Inc.*, 13 F.3d 633, 636 (2d Cir.1994)

("The crime-fraud exception strips the privilege from attorney-client communications that 'relate to client communications in furtherance of contemplated or ongoing criminal or fraudulent conduct.' " (quoting*In re Grand Jury Subpoena Duces Tecum Dated September 15, 1983,* 731 F.2d 1032, 1038 (2d Cir.1984))).

[12] "A party wishing to invoke the crime-fraud exception must demonstrate that there is a factual basis for a showing of probable cause to believe that a fraud or crime has been committed and that the communications in question were in furtherance of the fraud or crime." *United States v. Jacobs,* 117 F.3d 82, 87 (2d Cir.1997). It is not enough to show merely that privileged communications "might provide evidence of a crime or fraud." *In re Richard Roe, Inc.,* 168 F.3d 69, 71 (2d Cir.1999). "Rather, the communication itself must have been in furtherance of a fraud or crime and must have been intended to facilitate the fraud or crime." *Shahinian v. Tankian,* 242 F.R.D. 255, 258 (S.D.N.Y.2007) (citing *Jacobs,* 117 F.3d at 88).

***566** 1. *Application to E-mail 28*

[13] Having reviewed the contents of E-mail 28, the Court concludes that there is no evidence that it was sent in furtherance of a fraud or crime. The communication clearly addresses the legal issues which Fell and other Defendants face, and the advice is limited to addressing those legal issues, and indicates how Fell and other Defendants should respond to Brenner, with whom a legal conflict had arisen. The fact that the communication arose in the larger context of the Defendants' attempt to set up a competing business, and discusses matters which might, in Plaintiffs' eyes, constitute past criminal or fraudulent actions, does not transform this particular communication into one which furthers a crime or fraud. Accordingly, the Court concludes that E-mail 28 is protected by the attorney-client privilege, should be precluded from use by Plaintiffs, and should be returned to Defendants. Further, Plaintiffs should certify that all copies have been returned or destroyed. *See* Fed.R.Civ.P. 26(b)(5)(B).

2. *Application to All E-mails*

[14] Plaintiffs' crime-fraud exception argument is not limited, however, to only those e-mails for which attorney-client privilege was asserted. Plaintiffs also ask the Court to extend the principles underlying the crime-fraud exception to all of the e-mails in order to justify, and thereby excuse, Brenner's wrongful access to Fell's e-mail accounts. The Court declines to do so.

First, Plaintiffs' have not presented any authority for extending the crime-fraud exception beyond the borders of its standard application to material covered by the attorney-client privilege. Second, had Brenner waited and acted appropriately, she would have had access to all of Fell's e-mails, as well as all of the other Defendants' e-mails, in the normal course of pre-trial discovery. While Brenner's fears that Defendants might attempt to conceal evidence cannot, in this case, be written off as unfounded paranoia, neither federal law nor the Federal Rules of Civil Procedure can be ignored simply because a party believes herself to be wronged by the actions of a dishonest person. If the Court were to adopt Plaintiffs' suggestion, the crime-fraud exception would engulf all of the rules designed to ensure orderly and legal discovery of evidence, and could be invoked to justify any party's resort to illegal, extra-judicial measures to secure evidence. Accordingly, the Court rejects Plaintiffs' suggestion that the crime-fraud exception should excuse Brenner's violations of the SCA.

III. *Spoliation*

Defendants' final argument is that Plaintiffs' initial production of the e-mails, with their print date obscured, amounts to spoliation of evidence, justifying sanctions, including preclusion. The Court does not agree,

[15] " 'Spoliation is the destruction or significant alteration of evidence, or failure to preserve property for another's use as evidence in pending or reasonably

foreseeable litigation.' " *Allstate Ins. Co. v. Hamilton Beach/Proctor Silex, Inc.*, 473 F.3d 450, 457 (2d Cir.2007) (quoting *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir.1999)). Typically, when evidence is spoiled, a party requests dismissal or an "adverse inference" instruction to counteract the fact that the evidence is no longer available. *See West*, 167 F.3d at 780 (noting that dismissal is not the only sanction for spoliation, and that other sanctions, including jury instructions, also serve to vindicate the prejudice suffered by a party due to spoliation); *cf.* ***567***Residential Funding Corp. v. Degeorge Fin. Corp.*, 306 F.3d 99, 106 (2d Cir.2002) (noting that "adverse inference instruction [s] [are] usually [ ] employed in cases involving spoliation of evidence"). This is not, however, a typical case, because the evidence is available in its original form. Accordingly, neither of these severe sanctions—dismissal or an adverse inference instruction—are commensurate or appropriate sanctions.

[16] When the nature of the breach is non-production of evidence, as opposed to actual destruction or significant alteration, a district court "has broad discretion in fashioning an appropriate sanction". *Residential Funding Corp.*, 306 F.3d at 107. In *Residential Funding*, a case similar to this case, the plaintiff did not destroy "the e-mails on the back-up tapes. Rather, [the plaintiff] failed to produce the e-mails in time for trial." *Id.* at 106. The Second Circuit remanded the case, and instructed the district court to consider lesser sanctions, including awarding costs, if it determined that the defendant was not prejudiced by the delay. *See id.* at 112. Thus, the harm caused by delay in production is a relevant factor in determining sanctions, if a court determines that sanctions are warranted. *See West*, 167 F.3d at 780 (noting that addressing prejudice is an important aim of sanctions imposed for abuses of discovery).

[17] In this case, the original e-mails were not destroyed or altered, and Defendants inspected them prior to making their final argument to the District Court, regarding the motion for a preliminary injunction. The date the e-mails were printed was made known to Defendants and the Court before the preliminary injunction hearing. Thus, at most, Defendants could argue that production was delayed. However, Defendants were not harmed by the delay, as they were not prevented from addressing the evidence or making any arguments related to the e-mails—including the current preclusion motion.[FN10] *Cf. Residential Funding Corp.*, 306 F.3d at 107.

FN10. Defendants only claim as to the relevance that the obscured dates would have to their claims is that the dates the e-mails were printed might show contemporaneous "interception" under the ECPA. However, the Court has concluded that the ECPA does not apply to delivered e-mails, and the date the e-mails were printed is not relevant to the analysis because only delivered e-mails could be printed.

This is not to say that altering evidence, as Plaintiffs did, and delaying production of unaltered evidence until the day of the hearing, is excusable. However, Plaintiffs' current counsel has represented that prior counsel provided the e-mails in the state court litigation, and was responsible for obscuring the dates. (*See* Tr. at 14–15.) His explanation for doing so is unknown. Accordingly, the Court finds that obscuring the dates, alone, does not amount to spoliation warranting the imposition of sanctions, let alone total preclusion.

IV. *Remedies*

A. *Authority to Impose Sanctions*

The SCA allows a person who is "aggrieved by any violation of this chapter" to obtain "such relief as may be appropriate" in a civil cause of action. 18 U.S.C. § 2707(a). The statute further provides in

sub-section (b): "appropriate relief includes—(1) such preliminary and other equitable or declaratory relief as may be appropriate; (2) damages under subsection (c); and (3) a reasonable attorney's fee and other litigation costs reasonably incurred." *Id.* However, Defendants have not asserted a claim under the SCA; therefore, these provisions do not define or limit the sanctions the Court may impose in this case. Rather, Defendants appeal to the Court's inherent equitable authority to ***568** fashion appropriate sanctions for Brenner's actions.

[18][19] Federal courts do have "inherent 'equitable powers of courts of law over their own process, to prevent abuses, oppression, and injustices,' " *International Prods. Corp. v. Koons*, 325 F.2d 403, 408 (2d Cir.1963) (quoting *Gumbel v. Pitkin*, 124 U.S. 131, 144, 8 S.Ct. 379, 31 L.Ed. 374 (1888)); *see also Schlaifer Nance & Co., Inc. v. Estate of Warhol* 742 F.Supp. 165, 166 (S.D.N.Y.1990) (quoting *Koons*). Courts may impose sanctions and rely upon their inherent authority even "where the conduct at issue is not covered by one of the other sanctioning provisions." *Chambers v. NASCO, Inc.*, 501 U.S. 32, 50, 111 S.Ct. 2123, 2135, 115 L.Ed.2d 27 (1991). Furthermore, a district court may resort to its "inherent power to fashion sanctions, even in situations similar or identical to those contemplated by [a] statute or rule." *DLC Mgmt. Corp. v. Town of Hyde Park*, 163 F.3d 124, 136 (2d Cir.1998) (citing *Chambers*).

[20] In this situation, the sanctions available under the Federal Rules of Civil Procedure are not directly applicable, since Brenner's misconduct occurred prior to the filing of the litigation and outside the normal discovery process, and did not violate any court orders. *See Fayemi v. Hambrecht and Quist, Inc.*, 174 F.R.D. 319, 325 (S.D.N.Y.1997)(concluding that the Federal Rules of Civil Procedure did "not provide the authority for regulating the use of information obtained by a party independent of the discovery process"). Nonetheless, as the court in *Fayemi* found, pursuant to "its inherent equitable powers to sanction a party that seeks to use in litigation evidence that was wrongfully obtained," the court may preclude the use of stolen evidence in litigation, notwithstanding the fact that it would have been otherwise discoverable. *See id.* at 325–26.

In another analogous case, *Herrera v. The Clipper Group, L.P.*, Nos. 97 Civ. 560 & 561(SAS), 1998 WL 229499 (S.D.N.Y. May 6 1998), the defendant sought to preclude the plaintiff from using at trial documents improperly obtained outside the discovery process. Relying on its inherent authority, the court concluded that the plaintiff acted in bad faith and imposed sanctions, consisting of payment of costs and fees. *See id.* at *3 However, because the plaintiff could have properly obtained the evidence through the discovery process, the court declined to preclude the use of the evidence. *See id.* at *5. The court was also hesitant to provide the defendants with a "windfall" strategic advantage at trial. *See id.*

B. *Bad Faith*

The Second Circuit "has required a finding of bad faith for the imposition of sanctions under the inherent power doctrine." *Herrera*, 1998 WL 229499, at *4 (citing *United States v. Int'l Bhd. of Teamsters*, 948 F.2d 1338, 1345 (2d Cir.1991)). The Court concludes that Brenner acted in bad faith. The Court understands Brenner's impulse to unearth evidence of her disloyal employees' betrayal, after having reason to believe they had stolen important business documents and plans, and after they opened up a competing business after leaving PPBC. This is particularly true in light of Belliard's decision to invade her office, shred his non-compete agreement, and take other actions which caused Brenner to believe that he stole PPBC's client list, including e-mail addresses and telephone numbers.

But it is precisely this conduct which is the subject of this litigation and for which, if proved, Brenner has adequate legal remedies. Her actions—accessing of Fell's Hotmail account, and using that access to

open his Gmail account, and then resorting ***569** to "guessing" a password in order to gain access to Fell's WFBC account—violated federal law and offend general notions of personal privacy. Furthermore, her use of that information in this litigation taints the judicial process. Thus, even though Brenner's improper actions took place prior to the filing of the litigation, the fruits of Brenner's improper conduct have been heavily relied upon by Plaintiffs in pleading and arguing the merits of their case. The Court may therefore fashion sanctions for Brenner's wrongful access to Fell's personal e-mail accounts. *See Herrera,* 1998 WL 229499 at *5.

C. *Sanctions*

Defendants seek the complete preclusion of all of the e-mails, including their use in support of motions, at trial, and even for impeachment purposes. There are a variety of options, however, that are available to the Court.

On the mild side of the spectrum, the Court could preclude the use of e-mails obtained from Fell's accounts, but not e-mails properly obtained in the course of discovery from other Defendants or parties—even if the permitted e-mails might, in actuality, be the same as those precluded. Although this would amount to imposing almost no sanction, it recognizes the fact that the evidence would be otherwise discoverable.[FN11]

> FN11. In the Fourth Amendment context, the Independent Source Exception and the Inevitable Discovery Exception both allow evidence otherwise illegally obtained to be admissible in a criminal case if it could and would have been lawfully obtained anyway. *See Murray v. United States* 487 U.S. 533, 108 S.Ct. 2529, 101 L.Ed.2d 472 (1988); *Nix v. Williams,* 467 U.S. 431, 104 S.Ct. 2501, 81 L.Ed.2d 377 (1984).

However, the notion that the evidence would be otherwise discoverable also cuts in the other direction. Had Brenner allowed the litigation process to move forward, and not violated federal law to by-pass the rules of discovery, she could have properly obtained the e-mails in question. Moreover, many of the e-mails in issue were authored by other people and sent to Fell, and in those cases, those individuals were also aggrieved by Brenner's intrusion into Fell's e-mail accounts. Permitting precluded e-mails to be admitted from other sources would therefore fail to take into account the fact that Brenner's actions also violated the privacy rights of everyone with whom Fell communicated. As discussed, parties should not be excused from complying with the law and following the rules because of outrage, legitimate or otherwise, over another party's actions.

On the harsh side of the spectrum, the Court could completely preclude use of the e-mails for all purposes, in any context, regardless of whether they could be secured from some other source. This option could be tempered, however, by allowing the e-mails to be used for impeachment purposes.[FN12] Thus, while precluding the use of the e-mails as affirmative evidence, the Court would not permit Fell or others to testify falsely, or open the door to a line of testimony that is contradicted by the e-mails, knowing that the e-mails could not be used to impeach or rebut their testimony. Additionally, if there are e-mail chains between Defendants that merely contain a precluded e-mail from Fell, the chain of ***570** conversation would be admissible, and only the precluded e-mail would be redacted.

> FN12. Defendants urge the Court to reject an impeachment exception to preclusion, and cite to a Sixth Circuit case which explicitly holds that the ECPA does not provide for one. *See United States v. Wuliger,* 981 F.2d 1497, 1506 (6th Cir.1992). As the Court has determined that the ECPA does not apply, and the remedies available under the SCA are left to the discretion of the Court, and as this

> Court is acting pursuant to its inherent authority, nothing prevents the Court from allowing an impeachment exception.

Alternatively, selective preclusion of the e-mails could also be accomplished by carving out categories of e-mails. For example, e-mails dated before March 16, 2008, the last date of Fell's employment with PPBC, could be allowed in evidence, but later e-mails could be precluded; in fact, Defendants recognized this categorical distinction during oral argument. (*See* Tr. at 27.) Alternatively, only Gmail and WFBC account e-mails could be precluded, but not Hotmail account e-mails, since Fell clearly accessed his Hotmail account on Plaintiffs' computers and left his Hotmail password on PPBC's computers. Limited preclusion, such as one based on the date on which the e-mail was written (for example, e-mails sent after Fell left PPBC), or the type of account from which it was retrieved (e-mails from the Gmail or WFBC accounts), might be justified by the fact that both parties appear to have "unclean hands;" such a sanction would punish Brenner's wrongful acts, while limiting an evidentiary "windfall" going to Defendants, who also engaged in wrongful behavior. *See Fayemi,* 174 F.R.D. at 326 (permitting evidence that would otherwise have been precluded because of the "unclean hands" of the aggrieved party); *Herrera,* 1998 WL 229499, at *5 (declining to grant opposing party an evidentiary "windfall").

The problem with this alternative is that, ultimately, there is little justifiable basis to distinguish the e-mails according to their source or date. Brenner was not authorized to access *any* of Fell's e-mails directly from accounts maintained by third-party electronic communication service providers. Thus, while it is possible to create categories of e-mails, it is difficult to justify why one category should be precluded, while another should be admissible.

Finally, the Court could impose financial sanctions such as payment of the costs and fees incurred in bringing the instant motion.[FN13] These could be imposed in conjunction with a preclusion sanction, or, as the court did in *Herrera*, as an alternative to preclusion. Monetary sanctions, as opposed to full preclusion, would serve the Court's interest in favoring full disclosure of evidence. In the context of lifting a protective order, the Second Circuit has noted that "full disclosure of all evidence that might conceivably be relevant [is an] objective represent[ing] the cornerstone of our administration of civil justice." *Martindell v. International Tel. and Tel. Corp.,* 594 F.2d 291, 295 (2d Cir.1979).

> FN13. Defendants have not specified precisely the costs or fees they are seeking. The SCA permits awarding fees and costs, and, if the violation was willful, the imposition of punitive damages. *See* 18 U.S.C. § 2707(c); *see also Wyatt Technology Corp.,* 2006 WL 5668246, at *9 (awarding punitive damages to a counter-claimant under the SCA, because the plaintiff accessed the defendant's personal e-mail on a private foreign server, monitored the personal e-mail account, and did not obtain the defendant's authorization to do so).

The disadvantage of imposing a monetary sanction is that it does not really address the underlying injury to Fell's privacy. Furthermore, preclusion of the e-mails is the remedy most compatible with maintaining the integrity of the litigation process. As one court noted: "The [c]ourt is concerned with preserving the integrity of this judicial proceeding. What matters is balancing the scales. That can be done by prohibiting [a party] from making any use of the [wrongfully obtained] documents ...." *In re Shell Oil Refinery,* 143 F.R.D. 105, 108–09 (E.D.La.1992).

CONCLUSION

In fashioning a remedy pursuant to its inherent equitable powers, the Court has a great deal of discretion. *See* ***571***DLC Mgmt.,* 163 F.3d at 136

(upholding sanctions imposed by Magistrate Judge pursuant to the court's inherent equitable authority) (citing *Sassower v. Field*, 973 F.2d 75, 80–81 (2d Cir.1992)). The selection of a remedy for Brenner's actions is not, however, an easy task. Brenner wrongfully obtained Fell's e-mails, and her actions amount to a violation of the SCA. But the Court also recognizes that Brenner was reacting to what she perceived as Defendants' betrayal, theft of her property, and breaches of their fiduciary duties. Thus, the parties seeking equitable relief, Defendants, stand accused of having extremely unclean hands themselves. Furthermore, although Brenner's actions may have given Plaintiffs an advantage at the outset of this litigation, they did not, in the end, give them an advantage over Defendants they would not otherwise have had—all of the e-mails at issue here, except the one protected by the attorney-client privilege, would have been secured through the normal discovery process.

Nevertheless, at this stage in the litigation, the Court has not resolved the merits of Plaintiffs' claims, which will determine just how much dirt is on Defendants' hands. While the day may come when Defendants will face the consequences for their alleged misconduct, Brenner's wrongdoing has been established, and should not be counter-balanced by, as-yet, unproven allegations of wrongdoing on the part of Defendants. Accordingly, the imposition of sanctions against Plaintiffs is justified.

In the end, the one thing that should remain unsullied is the integrity of the judicial process. In this Court's view, that integrity is threatened by admitting evidence wrongfully, if not unlawfully, secured. *See REP MCR Realty, L.L.C. v. Lynch*, 363 F.Supp.2d 984, 1012 (N.D.Ill.2005) (“ ‘Litigants must know that the courts are not open to persons who would seek justice by fraudulent means.’ ”) (quoting *Pope v. Federal Exp. Corp.*, 138 F.R.D. 675, 683 (W.D.Mo.1990)). Therefore, in light of the unique circumstances of this case, the Court recommends that the e-mails be precluded from use in the litigation, but not for impeachment purposes should Defendants open the door. The Court also recommends that Plaintiffs should return or destroy all copies of E-mail 28, and so certify.

Pursuant to 28 U.S.C. § 636(b)(1)(C) and Rule 72 of the Federal Rules of Civil Procedure, the parties shall have ten (10) days from service of this Report to file written objections. *See also* Fed.R.Civ.P. 6(a) and (d). Such objections shall be filed with the Clerk of the Court, with extra copies delivered to the chambers of the Honorable John H. Koeltl, United States District Judge, and to the chambers of the undersigned, Room 1660. Any requests for an extension of time for filing objections must be directed to Judge Koeltl. Failure to file objections will result in a waiver of those objections for purposes of appeal. *See Thomas v. Arn*, 474 U.S. 140, 145, 106 S.Ct. 466, 470, 88 L.Ed.2d 435 (1985); *Frank v. Johnson*, 968 F.2d 298, 300 (2d Cir.1992); *Small v. Sec'y of Health & Human Servs.*, 892 F.2d 15, 16 (2d Cir.1989).

August 22, 2008.

S.D.N.Y.,2008.
Pure Power Boot Camp v. Warrior Fitness Boot Camp
587 F.Supp.2d 548

END OF DOCUMENT