Privacy & Data Security Law Journal

April 2008

Attorney-Client Communications Sent Over Employer E-Mail Systems May Not Be Privileged

ANTHONY P. SCHOENBERG

The author examines recent cases holding that e-mail communications with an attorney or spouse were not privileged because they were sent from a work-issued computer or e-mail account and also examines the prior law addressing these issues. This article offers suggestions and observations for attorneys and business people who may be impacted by these decisions.

In several recent decisions, courts in New York have concluded that e-mail communications with an attorney or spouse were not privileged because they were sent from a work-issued computer or e-mail account. Prior opinions addressing this issue have generally refused to eliminate privileges simply because a person communicates over a work-issued computer or e-mail account. While it is too early to tell whether these recent cases are indicative of a sea change in the law of privilege, at a minimum they demonstrate an increased willingness on the part of courts to eliminate privileges in cases where an employee knows or has

Anthony Schoenberg, a lawyer with Farella Braun + Martel LLP, maintains a broad-based commercial litigation practice focusing on complex business matters. He represents business entities in trade secret actions, fraud and business tort cases, real estate disputes, and construction disputes, among others. Mr. Schoenberg can be reached at aschoenberg@fbm.com.

reason to know — by virtue of an employer policy or flash-screen notice — that e-mails sent over a work-issued computer or e-mail account are not confidential. This article examines these recent cases and the prior law addressing these issues, and it offers suggestions and observations for attorneys and business people who may be impacted by these decisions.

RECENT NEW YORK DECISIONS

In *Scott v. Beth Israel Medical Center Inc.*,[1] a New York trial court held that a doctor's e-mails with his personal attorney were not sent in confidence — and, therefore, were not privileged — because they were sent over the employer's e-mail system. The court focused its analysis on the fact that the employer had a "no personal use" e-mail policy, which expressly barred employees from using their work e-mail for personal business. The court reasoned that the effect of this policy was to have the employer "looking over your shoulder each time you send an e-mail."[2] As a result, the court found that the e-mails were not confidential and, therefore, not privileged. Although the doctor claimed he was unaware of the policy, the court held that he had constructive notice of the policy because he was a hospital administrator and the hospital disseminated the policy to its employees.

In a more recent case, *United States v. Etkin*,[3] the Southern District of New York applied a similar analysis to the marital privilege. The court held that an e-mail from a criminal defendant to his spouse was not protected by the marital privilege because the defendant sent the e-mail from his work computer. The work computer contained a flash-screen notice, which appeared each time the defendant logged onto his computer, warning that his use of the computer constituted express consent for his employer to monitor his e-mail and that he had no expectation of privacy while using the computer. When the flash-screen notice would appear, the defendant had to click "OK" or "Enter" to complete the log on process. According to the court, this rendered the e-mail nonconfidential because "[b]y virtue of the log-on notices, Defendant is properly charged with knowledge of the fact that any email he sent to his wife computer could be read by a third party."[4] Although this case addressed the mari-

Published in the April 2008 issue of Privacy & Data Security Law Journal.

tal privilege and not the attorney-client privilege, both privileges are based on the notion of confidentiality. Accordingly, this case has clear implications for the attorney-client privilege.

PRIOR CASE LAW

Prior to *Scott* and *Etkin*, courts had been reluctant to eliminate the attorney-client privilege simply because an employee had used a work-issued computer or e-mail account to communicate with his or her lawyer. For example, in *In re Asia Global Crossing, Ltd.*,[5] the court held that e-mails sent by officers of a corporation to their personal attorney using their work e-mail accounts retained their privilege. The court observed that there was conflicting evidence about the existence of a corporate policy banning personal use as well as whether the officers were on notice of the corporation's e-mail policies. Consequently, the court refused to find that the officers' use of the corporation's e-mail system to communicate with their attorney eliminated the attorney-client privilege.

In *Curto v. Medical World Communications, Inc.*,[6] the court held that an employee did not waive the attorney-client privilege when she used an employer-issued laptop computer to send e-mails to her personal attorney via an Internet-based personal e-mail account. Although the employer had a policy prohibiting employees from using employer-issued laptop computers for personal business — a copy of which the plaintiff had signed — the court was unwilling to find a waiver of privilege because the policy was not enforced by the employer.

In California, *People v. Jiang*[7] dealt with a similar issue. In that case, the court addressed whether electronic documents prepared at the direction of a criminal defendant's attorney (and later printed out and transmitted by the defendant to the attorney) were privileged notwithstanding the fact that the defendant stored the documents on an employer-issued laptop computer. The prosecution argued that the documents were not confidential because the defendant had signed an "Employee Proprietary Information and Inventions Agreement," which gave the employer the right to inspect the laptop. The court, however, was persuaded that the documents were confidential because the defendant had made "substan-

tial efforts" to protect the documents by password protecting them and segregating them in a folder clearly marked as confidential. Moreover, the court was not persuaded that the "Employee Proprietary Information and Inventions Agreement" undermined the confidentiality of the documents, because it did not preclude personal use of the computer but, rather, was designed to protect the company's intellectual property. Although *Jiang* was depublished in 2005[8] and, thus, is not binding authority in California, it nevertheless provides a glimpse of how at least one California court has viewed these issues.

RELEVANT STATUTES

Several states have passed statutes that address the interplay between privilege and electronic documents, although interpretations of these statutes have varied. For example, in 2002, California enacted Evidence Code Section 917(b), which provides, "A communications…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."[9] In *Jiang*, discussed above, the court found that Section 917(b) supported its ultimate holding that the defendant's documents were privileged, explaining, "The Legislature's decision to mandate protection for electronic communication that necessarily may be accessible by third parties suggests that this type of access is not viewed by the Legislature as destroying the confidential nature of a communication."[10]

On the other hand, New York's Civil Practice Law and Rules Section 4548 is nearly identical to California Evidence Code Section 917(b), yet the courts in *Scott* and *Etkin* found that communications made over employer-provided e-mail systems (*Scott*) and computers (*Etkin*) were not privileged.[11] Thus, the existence of this type of statute does not necessarily dictate the result that a court will reach in a particular case.[12]

IMPLICATIONS FOR ATTORNEYS AND BUSINESSES

There are several practical lessons that can be drawn from these cases. The first lesson applies to attorneys representing individuals

employed by corporations or other entities. Such attorneys should avoid communicating with their clients via e-mail if their clients use work-issued computers or e-mail systems, since a court could potentially find that such e-mails are not privileged. If an individual client wants to communicate via e-mail, he or she should be instructed to do so from his or her personal computer over a personal e-mail account.

The second lesson is for policy makers at corporations and other entities. When crafting policies that govern employee use of entity computers and e-mail systems, policy makers should be aware that by including language advising employees that they do not have an expectation of privacy when using the entity's computers or e-mail systems — and/or advising them that such materials are subject to inspection by the entity —policy makers increase the likelihood that they would be able to discover an employee's communications with his or her attorney (because the communications might be deemed nonprivileged) in the event that the entity becomes involved in litigation with an employee. Flash screen notices may have a similar effect. While entities obviously may have other priorities or policy concerns that inform their decisions about how to craft computer and e-mail policies, the key point for purposes of this article is to make policy makers aware of these issues and, in particular, the fact that the contents of their policies might affect what is discoverable in litigation against current or former employees.

Finally, the last lesson is for attorneys who litigate cases on behalf of businesses or other entities against current or former employees. Attorneys litigating such cases should be aware that if the current or former employee attempts to make a claim of privilege with respect to e-mails or other materials that were sent over or maintained on the entity's computer or e-mail system, there may be a legal basis for testing the claim of privilege, particularly when litigating in New York.[13] Furthermore, as noted above, the contents of an entity's computer and e-mail policies can be crucial to a court's determination of such a claim.

CONCLUSION

The widespread use of e-mail has the potential to change some basic

assumptions about the meaning of a "confidential" communication. While it may seem apparent that an e-mail from a client to his or her attorney is privileged, that is not necessarily so, as the cases discussed in this article make clear. Furthermore, those cases are likely only the tip of the iceberg, as e-mail is now a firmly established part of how the world does business, and the law will continue to grapple with these issues in the future. Lawyers and business people would be well advised to stay on top of these issues as the legal landscape evolves in a rapidly changing world.

NOTES

[1] 847 N.Y.S. 2d 436 (N.Y. Sup. 2007).

[2] *Scott*, 847 N.Y.S. 2d at 440.

[3] Case No. 07-CR-913, 2008 U.S. Dist. LEXIS 12834 (S.D.N.Y. Feb. 20. 2008).

[4] *Etkin*, 2008 U.S. Dist. LEXIS 12834 at *16.

[5] 322 B.R. 247 (S.D.N.Y. 2005).

[6] 2006 WL 1318387 (E.D.N.Y. May 15, 2006).

[7] 131 Cal. App. 4th 1027 (2005), *depublished*, S136944, 2005 LEXIS 11250 (Sept. 28, 2005).

[8] *See People v. Jiang*, S136944, 2005 LEXIS 11250 (Sept. 28, 2005).

[9] Cal. Evid. Code § 917(b).

[10] *Jiang*, 131 Cal. App. 4th at 1054 n.16. The court noted, however, that the statute did not strictly apply to the communications at issue in *Jiang*, because the communications culminated in a non-electronic transmission from the defendant to his attorney. *Id.*

[11] Section 4548 provides, "[N]o communications 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." New York C.P.L.R. 4548 (McKinney 1999).

[12] Forming a backdrop to this issue is a line of cases addressing whether employees have an expectation of privacy in their computer files and e-mail. While the issue of privacy is doctrinally distinct from the issue of privilege, the privacy cases have informed the analyses that courts have applied in privilege cases. *See, e.g., In re Asia Global Crossing*, 322 B.R. at 257; *Scott*, 847 N.Y.S. 2d at 447 n. 5. In privacy cases, courts consider the following factors

in analyzing whether a person has an expectation of privacy in a work computer or e-mail account: (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? *See In re Asia Global Crossing*, 322 B.R. at 257. Courts have reached different results in privacy cases, sometimes finding that employees do have a right to privacy in work-issued computers and/or e-mail accounts and sometimes finding that they do not. In general, courts have been more likely to find that there is no expectation of privacy where the employer, either through its policies or otherwise, has put the employee on notice that use of the computer or e-mail system is not private and/or is subject to inspection. *Compare United States v. Simons*, 206 F. 3d 392, 398 & n. 8 (4th Cir. 2000) (no reasonable expectation of privacy in office computer and downloaded Internet files where employer had a policy of auditing employee's use of the Internet, and the employee did not assert that he was unaware of or had not consented to the policy); *Muick v. Glenayre Elecs*, 280 F. 3d 741, 743 (7th Cir. 2002) (no reasonable expectation of privacy in workplace computer files where employer had announced that he could inspect the computer); *Thygeson v. U.S. Bancorp*, 2004 U.S. Dist. LEXIS 18863, No. CV-03-467, 2004 WL 2066746, at *20 (D. Or. Sept. 15, 2004) (no reasonable expectation of privacy in computer files and e-mail where employee handbook explicitly warned of employer's right to monitor files and e-mail); *Kelleher v. City of Reading*, 2002 U.S. Dist. LEXIS 9408, No. Civ. A. 01-3386, 2002 WL 1067442, at *8 (E.D. Pa. May 29, 2002) (no reasonable expectation of privacy in workplace e-mail where employer's guidelines "explicitly informed employees that there was no such expectation of privacy"); *Garrity v. John Hancock Mutual Life Ins. Co.*, 2002 U.S. Dist. LEXIS 8343, No. Civ. A. 00-12143, 2002 WL 974676, at *1-2 (D. Mass. May 7, 2002) (no reasonable expectation of privacy where, despite the fact that the employee created a password to limit access, the company periodically reminded employees that the company e-mail policy prohibited certain uses, the e-mail system belonged to the company, although the company did not intentionally inspect e-mail usage, it might do so where there were business or legal reasons to do so, and the plaintiff assumed her e-mails might be forwarded to others) *with Leventhal v. Knapek*, 266 F. 3d 64, 74 (2d Cir. 2001) (employee had reasonable expecta-

tion of privacy in contents of workplace computer where the employee had a private office and exclusive use of his desk, filing cabinets and computers, the employer did not have a general practice of routinely searching office computers, and had not "placed [the plaintiff] on notice that he should have no expectation of privacy in the contents of his office computer"); *United States v. Slanina*, 283 F. 3d 670, 676-77 (5th Cir.) (employee had reasonable expectation of privacy in his computer and files where the computer was maintained in a closed, locked office, the employee had installed passwords to limit access, and the employer "did not disseminate any policy that prevented the storage of personal information on city computers and also did not inform its employees that computer usage and internet access would be monitored"), *vacated on other grounds*, 537 U.S. 802, 154 L. Ed. 2d 3, 123 S. Ct. 69 (2002); *Haynes v. Office of the Attorney General*, 298 F. Supp. 2d 1154, 1161-62 (D. Kan. 2003) (employee had reasonable expectation of privacy in private computer files, despite computer screen warning that there shall be no expectation of privacy in using employer's computer system, where employees were allowed to use computers for private communications, were advised that unauthorized access to user's e-mail was prohibited, employees were given passwords to prevent access by others, and no evidence was offered to show that the employer ever monitored private files or employee e-mails). *But see Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 101 (E.D. Pa. 1996) (no reasonable expectation of privacy where employee voluntarily sends an e-mail over the employer's e-mail system).

[13] Caution should be exercised in such cases to avoid running afoul of rules addressing the handling of another party's potentially privileged information. *See, e.g.*, Fed. R. Civ. Proc. 26(b)(5)(B) (information produced in discovery that is subject to a claim of privilege must be returned, sequestered, or destroyed by the receiving party, who must not use or disclose such information until the claim of privilege is resolved by the court); *State Comp. Insurance Fund v. WPS, Inc.*, 70 Cal. App. 4th 644, 656-657 (Cal. App. 1999) (if an attorney receives documents from an opposing party that appear to be privileged, attorney has an ethical obligation to refrain from examining the documents any more than necessary to determine they are privileged and must immediately notify opposing counsel and arrange for the return of the documents).