FARELLA BRAUN + MARTEL LLP

Privacy Law Basics and Best Practices

Information Privacy in a Digital World

Stephanie Skaff sskaff@fbm.com

What Is Information Privacy?

- Your name?
- Your phone number or home address?
- Your email address?
- Your password(s)?
- Your credit card number? Social Security number?
- Your financial information? Health information?
- Your location?
- Your online search history?
- Your private conversation? Email? IM?

Why Is Information Privacy Important To Your Business?

- According to Information Week, the amount of data captured and stored by businesses doubles every 12-18 months.
- Data is increasingly stored, shared and transferred in ways that can jeopardize security.
- Failure to protect sensitive consumer data can result in identity theft, harm to customers or employees, loss of consumer trust, and costly litigation.

Legal Standards

- Laws governing consumer data security:
  - Federal Trade Commission Act (FTC Act)
  - Fair Credit Reporting Act (FCRA)
  - FTC Disposal Rule
  - Industry-specific federal laws (e.g., HIPAA, GLB)
  - State data breach notification laws
  - Other state laws

Legal Standards

- The FTC Act prohibits “unfair or deceptive” practices.
  - Handle consumer information in a way that's consistent with your promises, including promises made in any written privacy policies.
  - Use reasonable measures to protect sensitive consumer data
    - PII – increasing amount of data is “sensitive”
    - “reasonable” – size, industry, collection and use, etc.

Legal Standards

- The Fair Credit Reporting Act (FCRA) governs the use and access to consumer reports
  - Written notification to individual, specific adverse action procedures.
  - Cal. Law Note: On October 10,2011, Governor Brown signed into law AB22, which further restricts the use of credit reports in the hiring and promotion process

Legal Standards

- The FTC Disposal Rule requires anyone who obtains a consumer report to use "reasonable" measures when disposing of it.
  - Businesses – no matter their size – must take steps to ensure that discarded customer information is not accessible to unauthorized persons

Legal Standards

- US Privacy Law is **Sectoral**
  - Examples of industry-specific laws and standards:
    - *Healthcare*: Health Insurance Portability and Accountability Act (HIPAA) imposes specific requirements on businesses that collect and use health information
    - *Financial*: The Gramm-Leach-Bliley (GLB) Privacy Rules and Safeguards Rule requires "financial institutions" to provide clear and conspicuous notice of data privacy practices and implement reasonable safeguards for customer data.
    - *Payment Card Industry*: PCI Data Security Standard

Legal Standards

- US Privacy law is **Decentralized**
  - 45 existing state information security and breach notification laws governing the response to and reporting of data breaches.
  - Cal. Civ. Code § 1798.80 et seq.
  - Federal “SAFE Data Act” would preempt the state laws and require implementation of information security programs and notification of affected individuals in the event of an information security breach

Legal Standards

- Examples of California laws:
  - First data breach law (Cal. Civ. Code § 1798.80)
  - Security of PII – reasonable, including contracts with third parties (Cal. Civ. Code §1798.81.5)
  - California "Shine The Light" Law
    - Businesses that share data with others for marketing purposes must provide a customer choice notice and disclosures regarding information sharing
  - California Online Privacy Protection Act (COPPA)
    - Businesses operating commercial Web sites or offering online services must post and comply with privacy policy that discloses what information is collected and how it is shared

Legal Standards

- US Privacy law is **Rapidly Developing**:
  - Personal Data Protection and Breach Accountability Act of 2011 (PDPBA Act) – significant penalties for data privacy and security violations, requirements for data storage and security auditing, broad enforcement powers, including private right of action for penalities up to $20 million per violation (recommended for Senate consideration)
  - “Commercial Privacy Bill of Rights (2011, Kerry and McCain) (in committee) – follows on Privacy by Design
  - SAFE data act (in committee)

Legal Standards

- US Privacy law is **Rapidly Developing**:
  - State laws with increasing granularity and scope:
    - Nevada – required encryption
    - Minnesota – incorporates parts of PCI standard
    - Massachusetts – overarching privacy statute, very detailed requirements

Privacy Principles

- Fair Information Principles:
  - Consent
  - Accountability
  - Identifying Purposes*
  - Collection Limitation
  - Use, Retention and Disclosure Limitation
  - Accuracy
  - Security
  - Openness
  - Access
  - Compliance

Privacy By Design (or Re-Design)

- Make Privacy A Company Priority
- Know Your Data Flow
- Manage Your Data Flow
  - Limit Collection, Access, Use and Retention
  - Collect, Store, Transfer and Dispose Securely
- Have A Written Privacy Policy and Follow It
- Conduct Ongoing Training and Oversight
- Develop a Data Incident Response Plan

Best Practice: Know Your Data Flow

- Conduct a Data Flow Audit to determine:
  - What information you **collect**;
    - Online and offline
  - Where it's **stored**;
    - Don't forget portable/mobile devices, offsite locations, third party vendors, cloud computing storage.
  - How it's **used;**
    - Shared with others? Transferred electronically?
  - How it's **disposed.**

Best Practice: Manage Your Data Flow – Limit Collection

- Examine your data flow to confirm that you are collecting only personal information that is necessary for business purposes.
  - Limit collection of Social Security numbers, which can be used by identity thieves to commit fraud. Only collect when needed, such as to report wages to the government or to seek a credit report.
  - Limit use of credit reports
  - Limit collection of other personal information that can trigger additional privacy requirements (e.g., financial and/or medical data)

Best Practice: Manage Your Data Flow – Increase Storage and Transfer Security

- Examine your data flow from collection to disposal. Determine who has access at each point and who should have access.
- Monitor computer systems to detect weaknesses or intrusions. Hacking and malware are leading causes of breaches.
- Review third party contracts to understand security protections.
  - Cloud computing
- Don't forget physical security
- Consider encryption for sensitive information

Best Practice: Manage Your Data Flow – Control Retention and Disposal

- Understand what information must be retained and for how long
  - Business, legal or contractual reasons for retention
- Ensure that private information leaving the company is not at risk of exposure
  - With retention requirements in mind, establish a policy and system for shredding, erasing or modifying records so that they are unreadable or indecipherable.

Best Practice: Have A Written Privacy Policy And Follow It

- Make sure your consumers and customers know what personal or sensitive information you collect, if and with whom you share the information, and how you safeguard the information.
  - Efforts to ensure privacy must be reasonable under the circumstances
  - If you say it, do it
  - Opt out requirements – CA customer choice notice

Best Practice: Ongoing Training And Oversight

- Use good hiring procedures and build information security training into orientation.
- Conduct additional training for your employees on privacy policies and procedures each year or whenever there is a material change in your business practices that could implicate the security of personal information.
- Oversee contractors and service providers.
  - Security audits, contractual provisions requiring protection, limits on collection and retention
- Measure compliance.

Best Practice: Develop An Incident Response Plan For Losses Of Personal Information

- Dedicated internal team in place, identified external resources;
- Identification and preservation of critical data and/or devices needed to investigate breach;
- Timely investigation of:
  - circumstances of the breach,
  - nature of the ongoing risk,
  - determination of what was exposed and whether notifications may be required.

FARELLA BRAUN + MARTEL LLP

Privacy Law Basics and Best Practices

Information Privacy in a Digital World

Stephanie Skaff sskaff@fbm.com