The Prevalence Of Privacy: Issues For In-House Counsel In The Information Age

Matthew Savare, Mary J. Hildebrand and Robert D. Chesler

LOWENSTEIN SANDLER PC

Matthew Savare

Mary J. Hildebrand

Robert D. Chesler

Virtually every company – large or small, private or public, local or national – is subject to a panoply of privacy laws. Privacy legislation in the United States is a complex and confusing patchwork of federal and state statutes and regulations. These laws, which govern a broad spectrum of commercial activities, are constantly evolving, particularly with the Obama administration's professed commitment to privacy.

An explication of the complexity and ubiquity of privacy regulations is beyond the scope of this article. Accordingly, the goal of this article is to provide the context within which privacy legislation is being drafted, recent developments in this area, and some guidance on how to mitigate your company's risks.

The Context

In his book *The Digital Person*, privacy scholar Daniel Solove describes how technology is enabling vast electronic databases to compile and store an unprecedented amount of personal information. Increasingly, these databases create detailed profiles of individuals, including their medical history, finances, purchases, activities, and interests. This data, which are collected when we make purchases, apply for a job, visit the doctor, make a phone call, or simply surf the Internet, are aggregated into what Solove calls "digital dossiers" and used in a variety of ways, including to process background and credit checks and to market products and services.

In this context, protecting consumer privacy is rapidly becoming one of the most significant legal and technological challenges facing government and industry. Unlike Europe, which has adopted a comprehensive privacy framework, America's federal legislation tends to focus on specific sectors. For example, the financial industry is regulated by the privacy and security provisions of the Gramm-Leach Bliley Act ("GLBA"), and the health care industry is governed by the Health Insurance Portability and Accounting Act ("HIPAA"), which was recently greatly expanded by the American Recovery and Reinvestment Act of 2009 ("ARRA").[1]

As described below, companies *outside* the financial and health care sectors must also comply with a variety of privacy regulations.

Specific Privacy Issues Of General Applicability

Although the following list is not exhaustive, it provides several important privacy regulations and concepts that affect virtually every business.

Data Breach Laws – In response to numerous data breaches, nearly every state, including New York, New Jersey, Pennsylvania, and Delaware and the District of Columbia, have enacted data breach notification laws. These laws, which extend beyond particular industries, require businesses to notify consumers of breaches of security. Many of these laws impose additional obligations on companies. For example, New Jersey's Identity Theft Prevention Act: (1) requires businesses to notify New Jersey consumers if their personal information has been compromised; (2) requires businesses to thoroughly destroy customer records that are no longer to be retained; (3) limits the use and display of social security numbers; and (4) allows consumers to place a security freeze on their consumer reports.

According to the Identity Theft Resource Center ("ITRC"), the number of data breaches at U.S. businesses, government agencies, and educational institutions increased by almost 50 percent from 2007 to 2008. The Ponemon Institute estimates that each compromised record costs the company who suffered the breach $202. Given that some breaches involve millions of records, such expenses, and the negative publicity surrounding the breach, could be devastating to a company. Shockingly, the ITRC found that only 2.4 percent of all security breaches in 2008 required the perpetrator to circumvent some type of encryption technology or other robust protection mechanism.

In January 2009, Heartland Payment Systems found evidence that malicious software had compromised card data that crossed its network. This incident, which is believed to be part of a global cyberfraud operation, is considered the largest data breach in U.S. history. Less than a month after reporting the breach, Heartland was sued for damages resulting from the alleged "inexplicable delay, questionable timing, and inaccuracies concerning the disclosures" with regard to the data breach.

Protection of Social Security Numbers – Many states, including New York and New Jersey, have passed statutes aimed to protect the social security numbers of consumers and employees. For example, the New York Social Security Number Protection Law prohibits companies from, among other things: (1) making an individual's unencrypted social security number available to the general public; (2) printing an individual's social security number on any card or tag required for the person to access products, services, or benefits provided by the company; (3) requiring an individual to transmit his or her social security number over the Internet, unless the connection is secure or the number is encrypted; (4) requiring an individual to use his or her social security number to access an Internet web site, unless a password, PIN, or other type of authenticating device is also required for the person to access the web site; and (5) printing an individual's social security number on any materials that are mailed to the person, unless a state or federal law requires the number to be on the document being mailed.

In addition, the law also requires any company in possession of an individual's social security number to: (1) take reasonable precautions to ensure that none of the company's officers or employees has access to the SSN for any purpose "other than for a legitimate or necessary purpose related to the conduct of such business or trade," and (2) provide safeguards "necessary or appropriate" to prevent unauthorized access to the SSN and protect its confidentiality.

Similarly, the New York Employee Personal Identifying Law prohibits employers from communicating to the public an employee's "social security number, home address or telephone number, personal electronic mail address, Internet identification name or password, parent's surname prior to marriage, or drivers' license number." Specifically, the law prohibits employers from: (1) publicly posting or displaying an employee's social security number; (2) visibly printing a social security number on any identification badge or card, including time cards; (3) placing a social security number in files with unrestricted access; and (4) communicating an employee's personal identifying information to the public.

Adherence to Privacy Policy – Virtually every business has a web site. And, although required only for financial institutions, entities covered by HIPAA, and web sites governed by the Children's Online Privacy Protection Act ("COPPA"),[2] many of these web sites contain a privacy policy. Unfortunately, many companies consider their privacy policy to be a form document and do not tailor it to suit their particular circumstances. Such an attitude could have significant ramifications.

For example, the now-defunct Internet store Toysmart.com had a privacy policy posted on its web site that claimed the retailer would not sell any data it collected concerning its customers. After the company declared bankruptcy in 2000, it attempted to sell its consumer data as a standalone asset. The Federal Trade Commission ("FTC") sued Toysmart.com, alleging that such a sale would contravene the privacy policy and thus constitute an unfair or deceptive act or practice under the FTC Act. Given that the principal asset of many companies, particularly Internet retailers, is their data, companies should craft their privacy policies in such a way to provide them maximum flexibility in the event of a sale, merger, or bankruptcy.

Similarly, in February 2009, CVS Caremark settled a privacy dispute with the FTC. The FTC had alleged that CVS violated the promise it made in its privacy policy that "nothing is more central to [CVS'] operations than maintaining the privacy of your health information," when CVS was found discarding into open dumpsters sensitive information (such as patient names, prescription information, credit card information, and social security numbers). In a separate but related settlement, CVS agreed to pay $2.25 million for HIPAA violations.

Behavioral Advertising – One of the more controversial privacy issues is the practice of behavioral advertising, which is the tracking of consumers' Internet surfing to create and serve tailored advertisements. This practice has received increased scrutiny from the government and privacy advocates over the last year and has resulted in at least one class action lawsuit alleging privacy violations.

To date, the FTC has allowed the advertising industry to self-regulate the practice. These self-regulatory guidelines call for: (1) greater disclosure and transparency to consumers of a company's data collection and use practices; (2) consumers to have the right to opt out of such data collection; (3) obtaining consent before collecting sensitive information; and (4) companies' honoring their promises regarding the collection and use of such data.

Risk Mitigation Principles

Given the myriad privacy statutes currently in effect, there is no single compliance checklist. However, the following principles are useful when analyzing your company's exposure to privacy claims:

1. To the greatest extent possible, companies should employ the principles of data minimization (*i.e.*, collecting only data that is actually necessary to conduct their businesses) and retention limitation (*i.e.*, promptly and securely destroying data that is outdated or no longer needed).

2. Companies should adopt and implement robust electronic and physical safeguards to protect and monitor their consumers' and employees' personal information. Filing cabinets containing sensitive information should be locked; all computers, laptops, and networks should be password protected; and electronic data, particularly data stored on laptops and networks, should be encrypted using industry-standard protocols.

3. All paper and electronic files that are to be discarded should be obliterated. For example, paper documents should be cross-shredded or destroyed by a third-party vendor; removable media such as thumb drives or CDs should be thoroughly destroyed, not simply erased or reformatted.

4. Companies should create strict internal procedures that dictate how they will respond to security breaches.

5. Companies using outside vendors to collect, store, process, transmit, or destroy their data should: (i) investigate and determine if their vendor's privacy and security policies and practices are adequate; (ii) delineate the vendor's specific obligations, rather than simply stating that the vendor will comply with all applicable laws; (iii) perform privacy audits on the potential and existing outsourcers on a periodic basis; and (iv) attempt to establish a strong working relationship with the vendor's privacy officer.

6. Companies should consider obtaining cyber-insurance, which covers a broader range of privacy and identity theft claims than general liability policies.

***Matthew Savare** practices intellectual property, media, and entertainment law with Lowenstein Sandler PC. **Mary J. Hildebrand** is a senior Member of Lowenstein Sandler PC, focusing her practice on the commercialization of intellectual property including outsourcing, licensing, data privacy and security. **Robert D. Chesler** is a senior Member of Lowenstein Sandler PC, and Chair of the firm's Insurance Practice Group. He represents policyholders in a broad variety of coverage claims against their insurers, and advises companies with respect to their insurance programs.*

[1] *For example, ARRA applies HIPAA's privacy rules to the "business associates" of covered entities and other heretofore non-covered entities; it allows patients to pay for health care services out-of-pocket and request non-disclosure of the service; authorizes increased penalties for HIPAA violations; and imposes greater restrictions on certain sales and marketing of protected health information.*

[2] *COPPA applies to (1) operators of commercial web sites that are geared to children under 13 and collect personal information from the children, (2) operators of general audience web sites that knowingly collect personal data from children under 13, and (3) operators of general audience web sites that contain a separate children's area and that collect personal data from children under 13.*

Please email the authors at msavare@lowenstein.com, mhildebrand@lowenstein.com or rchesler@lowenstein.com with questions about this article.