The Changing Data Privacy Landscape

Brought to you by *InsideCounsel* and Foley & Lardner LLP

"The Changing Data Privacy Landscape" was the topic of discussion during the May 22, 2007 presentation of The Web Conference Series for Corporate Counsel. *InsideCounsel* Editor-in-Chief Robert Vosper led the discussion. Mr. Vosper was joined by Foley Litigation Partners Andrew B. Serwin and Pamela L. Johnston. The panel discussed key privacy laws that can impact businesses as well as steps to take in the event of a security breach.

Addressing Trends

Privacy has become a far-reaching issue where a misstep can result in liability and bad publicity for a company. Federal, state, and international legislation in this area continues to evolve; companies should monitor all regulations that apply to their business and adapt organizational policies to remain compliant.

Sharing Solutions

Information Security and Privacy

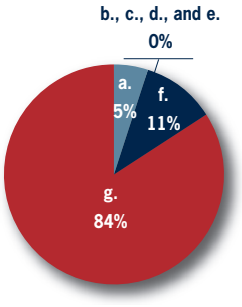
The general principles of information security and privacy include: notice, choice, onward transfer, access, security, data integrity, and enforcement. Four questions help to encapsulate privacy issues:

- What information does a company collect?
- What does the company do with the information?
- When can't a company disclose information?
- When must a company disclose information?

Polling Question*

Which of the following types of personally identifiable information does your company collect, utilize, or maintain in its files or on its computer system (including customer and/or employee data)?

a. Names, addresses, and e-mail addresses
b. Social Security Numbers (SSNs)
c. Credit card or bank account numbers
d. Health information/records
e. Dates of birth
f. More than one of the above
g. More than two of the above



Federal Privacy Statutes

- Children's Online Privacy Protection Act (COPPA)
- Gramm-Leach-Bliley Act (GLB), which addresses financial matters
- Electronic Communications Privacy Act (ECPA)
- Identity Theft and Deterrence Act
- Health Insurance Portability and Accountability Act (HIPAA), which addresses health care and medical matters
- Others, including Fair Credit Reporting Act (FCRA) and Fair and Accurate Credit Transactions Act (FACTA)

ECPA

ECPA (18 U.S.C. § 2510 *et seq.*), which can have implications for many businesses, is the main law at the federal level covering electronic communications. The act has two portions: the Stored Communications Act and the Wiretap Act.

The Stored Communications Act primarily deals with such communications as saved e-mails and voice messages.

The Wiretap Act applies to communications "on the wire," or being transmitted. The more restrictive of the two portions for most businesses, the Wiretap Act prohibits the "interception" of "electronic communications," which include "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce."

Most businesses encounter ECPA in the context of reviewing employee communications. Because violating ECPA is a federal felony, it is critical to be aware of its restrictions. Before reviewing employee communications, ensure that the situation falls into one of two exceptions that may protect a company against charges of fraudulent conduct:

- Reviewing the communications served to protect the provider, another provider, or a user from fraudulent, unlawful, or abusive use of such service
- Communications were reviewed by a person employed or authorized, or whose facilities are used, to forward such communication to its destination

Amended definitions of "wire communication" — such as those laid out in the USA PATRIOT Act — are important to note, as are additional restrictions upon "public" providers.

** All polling results are based upon the number of respondents to each question rather than the total number of participants in the Web conference.*

InsideCounsel | FOLEY
FOLEY & LARDNER LLP

State Employee e-Mail Monitoring Laws

Companies also should evaluate state laws before reviewing employee communications, as they may be more restrictive than federal regulations, and violations may result in civil penalties. For example, Connecticut requires notice as well as posting of notice of the employer's monitoring policies, while Delaware requires that notice be given every day to employees.

Randall David Fischer v. Mt. Olive Lutheran Church, et al. is one recent case highlighting the complicated issues involved in e-mail monitoring. In this case, an employer accessed an employee's private third-party Web-based e-mail account, which the employee accessed via the employer's network. The employer obtained the password through a keystroke logger. A court found enough evidence to go to trial over a potential wiretap violation. Because employees ostensibly would use personal e-mail accounts — rather than company e-mail systems — to send any company secrets, the issue of privacy relating to third-party accounts should be addressed in the employee handbook. Additionally, policies can be implemented to block access to such accounts.

FCRA and FACTA

FACTA is an amendment to FCRA that creates new rules regarding identity theft, particularly related to credit or security freezes. The panel stated that more than half of the states also have enacted security-freeze laws that — in their most restrictive forms — require a consumer reporting agency to put a hold on credit within 15 minutes.

FACTA's main impact on businesses that are not financial institutions is its Data Destruction Rule, which went into effect June 1, 2005. The rule requires the destruction of certain forms of personally identifiable data if they are a derivative of a consumer report; the Federal Trade Commission (FTC) may issue enforcement if adequate steps are not taken to destroy the data. This is important for businesses completing background checks on employees.

FACTA and Credit Card Numbers

A number of new laws went into effect on January 1, 2007 regarding credit card receipts. FACTA prohibits displaying more than the last five numbers of the credit card or the expiration date. Certain state laws are more restrictive, so companies doing business across state lines or via the Internet should ensure compliance with all applicable laws.

Bankruptcy Reform Act of 2005

Though the Bankruptcy Reform Act is not a privacy statute or act, per se, recent amendments to 11 U.S.C. § 363 can impact a company's privacy policy. Issues have arisen when bankrupted businesses attempt to sell personally identifiable information — often a company's main asset. Similar issues also can arise during a merger. The panel suggested posting a clear disclosure about the sale of personally identifiable information in the company privacy policy on its Web site.

Pretexting: A Federal Crime

According to 18 U.S.C. §1039, pretexting — or obtaining phone records information under false pretenses — is a federal felony. Additionally, it is illegal to knowingly and intentionally sell, buy, or transfer confidential phone records information. There also exist numerous state pretexting laws, a majority of which relate to phone records information.

Federal Disclosure Statutes

Federal disclosure statutes with which most businesses contend include:

- Communications Assistance for Law Enforcement — Requires telecommunication and Internet service providers to have a "back door" through which law enforcement agents are able to tap all types of communication
- USA PATRIOT Act — By amending existing laws and creating new ones, the act increases the ability of the government to obtain certain types of communication
- Digital Millennium Copyright Act — Criminalizes certain types of conduct related to copyright infringement and provides content owners the ability to obtain subpoenas in an abbreviated manner and timeframe

Employees and customers should be informed that disclosure statutes may compel a company to disclose information, as noncompliance could result in penalties, subpoenas, or court orders.

California Legislation

Even if companies operate outside the State of California, they likely have customers in or data originating from the state. Because the California authorities tend to remain vigilant, it is important for businesses to be aware of the legislation that impacts them. Additionally, many other states have replicated California laws with similar regulations.

California's Online Privacy Protection Act

California's Online Privacy Protection Act (Cal. Bus. & Prof. Code § 22579) applies if "personal information" is collected through a Web site. The act requires that a Web site:

- Display a privacy policy that discloses the type of information collected
- Describe the process, if any, for consumers to change their information
- Explain the process for consumers to receive notice of material changes to the policy
- Identify its effective date

Restrictions on the Collection of SSNs

As savvier consumers have become wary of providing personal information, protecting SSNs has become paramount to a company's data security practices. California's Civil Code § 1798.85 has been replicated across most states, with variations. According to California's code, companies cannot:

- Post or publicly display SSNs
- Print SSNs on identification cards
- Require people to transmit SSNs over the Internet unless data is encrypted or the connection is secure
- Use SSNs as logins unless passwords also are required
- Print SSNs on materials unless legally required

Data Security Law and Data Destruction Law

California established its Data Security Law (AB 1950 Cal. Civ Code § 1798.81.5), and other states have followed suit. It is a broad law that applies across the board, even to nonelectronic data, and is triggered if a business owns unencrypted personal data regarding a California resident. Businesses and third parties that receive data must have "reasonable" security measures and procedures.

California also enacted its Data Destruction Law, which requires that consumer records containing personal information be destroyed once the records are no longer needed. This obligation applies whether the record is in electronic or nonelectronic form. Destruction is accomplished through shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

Other Data Security/Destruction Laws

A partial list of other data security and data destruction laws includes: the Sarbanes-Oxley Act (SOX), with internal controls and data integrity, particularly as it relates to financial information; FACTA; and state laws enacted in Arkansas, California, Colorado, Indiana, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, Rhode Island, Tennessee, Texas, Utah, Vermont, and Washington.

Restrictions on Direct Marketing

California's civil code addressing direct marketing (Cal. Civ. Code §1798.83) holds that a business is under certain document retention and disclosure requirements if the business discloses "personal information" to third parties, and knows or reasonably should know that the third parties used the personal information for the third parties' direct marketing purposes. In California, a number of data are considered personal information, including number of children, height and weight, race, religion, bank or investment accounts, credit card balances, payment histories, information pertaining to the customer's creditworthiness, assets, income, or liabilities, and more.

The Importance of Opt-Outs

In California, if an opt-out mechanism is available, then these requirements do not apply. If a company is able to track consumers who have opted out, there is significantly more leeway in regard to direct mailing.

International Issues

SOX has raised issues for international companies that must comply with both SOX whistleblower requirements and the European Union (EU) directive. SOX requires an internal whistleblower process that guarantees the whistleblower will not be fired; he or she has many rights and the company is subject to criminal prosecution for violating those rights. This law essentially goes head-to-head with EU privacy laws, as it is seen as a violation of the privacy rights of the individual being targeted for investigation based upon an anonymous claim. While agencies such as the French data protection authority have provided some guidance, this remains an open issue of which companies doing business in the EU should be aware.

FTC Security Suggestions

The FTC — one of the leading federal agencies regulating security and privacy — has recommended several policies for maintaining up-to-date security for computer systems:

- Follow a written contingency plan to address any breaches of physical, administrative, or technical safeguards
- Regularly check with software vendors to obtain and install patches that resolve software vulnerabilities
- Use antivirus software that updates automatically
- Maintain up-to-date firewalls, particularly if using broadband Internet access
- Provide central management of security tools for employees and pass along updates about any security risks or breaches
- Plan ahead: Assume that you will need to access policies, notices, and resources after hours, when few people are available

FTC and Privacy

The FTC has an announced privacy agenda, which includes:

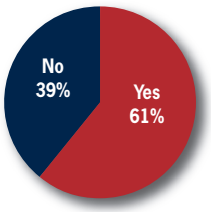
- Stepping up enforcement of spam laws
- Increasing assistance to victims of identity theft
- Enforcing companies' privacy promises
- Enforcing federal laws

In examining various enforcement actions brought against companies by the FTC, a discernable overarching principal is a concerted attempt to prevent consumer identity theft. Recent cases show a progression in enforcement, based on the premise that lack of data security is an unlawful

or unfair business practice — even if regulation does not specifically require data security measures.

Polling Question*

Are you worried that a breach of data security involving your company's private data will occur in the next 12 months?



Notice-of-Security-Breach Legislation

Current legislation — which can vary from state to state — addresses common issues that arise from a breach of security, including:

- When notice must be given
- Form of the notice
- To whom notice must be given
- Scope of federal preemption
- Effect of existing security policies

California, the City of New York, the Office of the Comptroller of the Currency (OCC), and about 35 other states have enacted laws or rules regarding notice of security breach. California Civil Code §1798.82 is triggered if there is a breach of a data security and a consumer's personal information is implicated. The act applies even if a reasonable belief that there was an acquisition of data exists. Though an aggressive law, other states may be even more stringent; it is important to track laws in all states in which a company operates.

Individual issues should be examined on a case-by-case basis, as varying legislation may impact companies differently depending on the situation. Companies should take stock of additional issues in light of the particular laws that affect them:

- Was the data encrypted? If so, the company may not be subject to giving notice.
- Was the data stored in electronic or nonelectronic format? Several state security-breach-notice regulations apply to both forms (e.g., North Carolina and Wisconsin).
- Is there a general duty to notify? As outlined above, failure to give notice in and of itself has been found to be an unfair business practice, even in the absence of a law requiring notice.
- Is notice required if there is no likelihood of identity theft? In some states it is; in others is it not.

Handling a Security Breach

In the event that a company experiences a breach of data or privacy, it must consider:

- Obligations to customers, employees, and the law
- Controlling the message
- When to go beyond what is required
- When to involve law enforcement

Because the situation initially might be confusing, it is important to get a handle on events as quickly as possible.

- If it is an option, contact the company privacy officer or counsel for guidance
- Preserve evidence, particularly items that easily or frequently are written over, including back-up tapes or logs
- Try to determine whether the company is experiencing an intrusion or theft
- Establish obligations at federal and state levels
- Consider contacting law enforcement

When to Contact Law Enforcement

Many companies are reluctant to contact law enforcement in the event of a breach of security. However, involving law enforcement can be useful, particularly when there is an intrusion or malicious internal breach. Agencies quickly can access external information that may be difficult for the company itself to obtain. This also helps to record key evidence before it disappears. The agencies also can apply penalties that aid in preventing another breach.

Contacting law enforcement agencies also can help with "spin control," enabling a company to announce publicly that it proactively has contacted the authorities, who are highly trained in handling these situations.

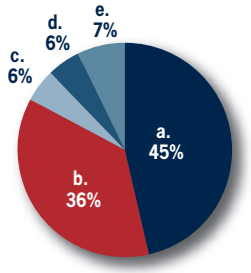
The panel recommended contacting federal agents first, as there exists a sophisticated network of agents and prosecutors dedicated to these issues. They can work with a company's information technology (IT) department to resolve the issue quickly and effectively. Federal agents also can refer companies to local departments with similar skills.

** All polling results are based upon the number of respondents to each question rather than the total number of participants in the Web conference.*

Polling Question*

Would you favor Congress passing a comprehensive federal statute that would preempt all state notice laws regarding breaches of consumer data if it required all companies to disclose all breaches of data security to consumers?

a. Strongly favor
b. Slightly favor
c. Neutral
d. Slightly disfavor
e. Strongly disfavor



Privacy Litigation

Many privacy cases fail due to a lack of damage, as was the case in the following matters:

- *In re Northwest Airlines Privacy Litigation, 2004* U.S. Dist. LEXIS 10580 (D.C. Minn. June 6, 2004)
- *Dyer v. Northwest Airlines Corporation, et al.,* 334 F.Supp.2d 1196 (D.N.D. 2004)
- *In re JetBlue Airways Corp. Privacy Litigation,* 379 F.Supp.2d 299, 2005 WL 1813273 (E.D.N.Y. July 29, 2005)

The panel suggested the possibility of a future increase in laws that do not require damage for a civil lawsuit, but that do have statutory penalties.

Summary

In order to navigate the myriad federal, state, and international security regulations successfully, a company must determine all applicable laws based upon the information it collects, where it does business, and the identity of its customers. Steps can be taken to mitigate risk, including:

- Assessing all information being collected and stored and eliminating all nonessential data
- Considering security measures of both the company and any third-party vendors
- Establishing after-hours access to policies and notices
- Ensuring privacy policies make the necessary disclosures
- Reserving the right to modify privacy policies
- Ensuring that employees are aware of privacy and security policies

In the event of a security breach, act immediately to preserve evidence before it disappears. Companies should investigate all obligations, and consider contacting law enforcement to aid in managing the situation.

Foley & Lardner LLP has compiled the 2006 series program summaries into an electronic brochure entitled *The Web Conference Series for Corporate Counsel — 2006 Year in Review*. To view and download a copy of the brochure, please visit **Foley**.com/webconference.

Please visit **Foley**.com/webconference for more information or to experience a recording of the "The Changing Data Privacy Landscape" conference.

Web conference services provided by:

Microsoft Office Live Meeting

** All polling results are based upon the number of respondents to each question rather than the total number of participants in the Web conference.*