GEORGETOWN UNIVERSITY LAW CENTER
CONTINUING LEGAL EDUCATION

CORPORATE COUNSEL INSTITUTE 2006

MARCH 9, 2006
Washington, DC

CURRENT LEGAL TRENDS IN INFORMATION PRIVACY AND DATA SECURITY

by

Lisa Jose Fales
and
Jennifer T. Mallon

Venable LLP
Washington, DC

INTRODUCTION

It is nearly impossible to read the newspapers over the past year without seeing a front-page headline announcing a significant security breach at a well-known company. A 2003 Federal Trade Commission ("FTC") survey found that nearly 10 million people, or nearly five percent of U.S. adults, have been victims of some form of identity theft. Those numbers translate into $48 billion in losses to businesses, $5 million in losses to victims, and almost 300 million hours lost trying to resolve the problems resulting from the identity theft.[1]

As consumers and businesses become increasingly concerned about privacy and the security of personal information, these issues have become hot button, high-profile issues with plenty of political appeal. Not surprisingly, Congress, the Federal Trade Commission, state legislatures, state attorneys general, and other federal and state governmental entities have made privacy and information security a top priority. As the number of investigations into breaches escalates, the federal and state governments are considering additional enforcement and legislation to ensure that privacy is protected. This paper discusses the current laws addressing information privacy issues and focuses on recent federal enforcement actions in this arena. In addition, it provides practical advice for corporate counsel to ensure corporate compliance with information privacy laws. It also includes practical advice on how to deal with a security breach, including ensuring that corporations have an incident response plan *before* a breach occurs since the question is not if a breach will occur - - but when.

WHAT IS INFORMATION PRIVACY LAW?

Information privacy is the expectation that confidential personal information disclosed with an expectation of privacy will not be revealed to unauthorized third parties. The basic concept is that an individual has an interest in controlling the collection, use, and disclosure and dissemination of personally identifiable information. It generally is recognized that individuals are not afforded protection for information that is publicly available or voluntarily disclosed in a public place.

The Restatement (Second) of Torts classifies four basic privacy rights:

1. Unreasonable intrusion upon the seclusion of another without consent;

2. Appropriation of a person's name or likeness;

3. Publication of private facts;

4. Publication that places a person in a false light.[2]

---

[1] SYNOVATE, FED. TRADE COMM'N – IDENTITY THEFT SURVEY REPORT 4-9 (Sept. 2003), http://www.ftc.gov/os/2003/09/synovatereport.pdf.

[2] RESTATEMENT (SECOND) OF TORTS §§ 652A.

OVERVIEW OF KEY LAWS ADDRESSING INFORMATION PRIVACY ISSUES

There are a number of federal laws that address information privacy. In addition, over the past two years, Congress has considered a large number of privacy and information security bills, none of which ultimately passed. These bills focused on the requirements for notification of consumers when their sensitive personal information has been compromised, [3] computer and internet collection of personal data, the protection of social security numbers, and the regulation of personal information brokers. Some of the key federal laws are described below:

- **Federal Trade Commission Act ("FTC Act"):**[4] Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[5] Under the FTC Act, the Commission is granted broad jurisdiction to prohibit unfairness and deception by enforcing companies' express or implicit privacy promises regarding collection, use, and security of consumers' personal information. The FTC has also used its Section 5 unfairness authority to determine whether a company's information security measures were reasonable and appropriate under the circumstances.

- **Telemarketing Rules issued by the FTC and Federal Communications Commission ("Telemarketing Rules"):**[6] In 2003, the FTC and Federal Communications Commission ("FCC") amended their respective rules regarding telemarketing. The revised telemarketing rules implemented the national do-not-call list ("DNC"). Consumers may enroll in the DNC via a web site or a toll-free number. Enrollment is effective for five years and may be renewed. Both the FTC and FCC allow exceptions for calls to consumers on the national DNC if the consumer purchased something from the calling company within the past 18 months or if the consumer initiated/applied to the company in the past three months (unless the consumer specifically requested that the company not call).[7]

---

[3] Emilio Cividanes, *US Data Security Developments*, DATA PROTECTION LAW & POLICY, Oct. 2005, at 13-14. (Attachment 1)

[4] 15 U.S.C. §§ 41-58.

[5] 15 U.S.C. § 45(a).

[6] 16 C.F.R. § 310, 47 C.F.R. § 64.1200.

[7] Political and charitable calls are exempt from the DNC.

In addition, the Telephone Consumer Protection Act[8] ("TCPA"), as amended by the Junk Fax Prevention Act, prohibits sending an "unsolicited advertisement" by fax unless the sender has an established business relationship with the recipient and the fax contains a disclosure notifying the recipient of the opportunity to opt-out of receiving future unsolicited fax advertisements from the sender. Unless the sender established a business relationship with the recipient prior to enactment of the Junk Fax Prevention Act, the statute further requires that the sender obtain the recipient's fax number either through the recipient's voluntary communication of such number, within the context of the established business relationship ("EBR"), or from a directory, advertisement or site on the Internet to which the recipient voluntarily agreed to make available its fax number for public distribution. If a "do-not-fax" request is received from a person or entity with whom the sender has an EBR, the sender must stop sending unsolicited advertisements by fax to the person or business who made the request. The penalty for *each violation* is $500 or up to $1,500 if a company willfully and knowingly violates the law.

- **The Privacy Act of 1974 ("Privacy Act"):**[9] The Privacy Act prohibits unauthorized disclosure of certain records maintained by the federal government pertaining to individuals. The Privacy Act also grants individuals the right to obtain a copy of one's own file and to learn whether personal records have been disclosed. The Privacy Act does not protect the privacy of records that are not maintained by the government. From a practical perspective, the Privacy Act is important for private companies that are government contractors.

- **Fair Credit Reporting Act ("FCRA"):**[10] FCRA, enacted in 1970, ensures the privacy of information contained in consumer reports through the regulation of credit bureaus, any entity or individual that uses credit reports, and the businesses that furnish information to credit bureaus. The FCRA requires that sensitive credit report information be used only for certain permitted purposes including in response to a court or subpoena in connection with proceedings before a federal grand jury; in accordance with written instructions from the consumer; for use in connection with a credit transaction; for employment purposes; for insurance underwriting; for eligibility for a license or other benefit granted by the government that considers an applicant's financial responsibility or status; for potential investors or servicers in connection with valuing the credit or repayment risks of an existing credit obligation; for an otherwise legitimate business need in connection with a transaction initiated by the consumer; or in response to a state or local child support enforcement agency.

[8] 47 U.S.C. § 227.

[9] 5 U.S.C. § 552a.

[10] 15 U.S.C. §§ 1681-1681v.

- **Gramm-Leach-Bliley Act ("GLB Act"):**[11] The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act, includes provisions to protect consumer and customer personal financial information maintained by financial institutions.[12] The GLB Act prohibits financial institutions from disclosing consumer or customer information to non-affiliated third parties without first allowing consumers the ability to opt out of the disclosure ("Financial Privacy Rule").

  The GLB Act also requires financial institutions to implement appropriate safeguards to protect the security and integrity of their customer information ("Safeguards Rule"). The Safeguards Rule applies to individuals or organizations that are significantly engaged in providing financial products or services to consumers, including check-cashing businesses, data processors, mortgage brokers, nonbank lenders, personal property or real estate appraisers, and retailers that issue credit cards to consumers. According to the Safeguards Rule, financial institutions must develop a written information security plan that describes their program to protect customer information. All programs must be appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue. Covered financial institutions must:: (1) designate the employee or employees to coordinate the safeguards; (2) identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of current safeguards for controlling these risks; (3) design a safeguards program, and detail the plans to monitor it; (4) select appropriate service providers and require them (by contract) to implement the safeguards; and (5) evaluate the program and explain adjustments in light of changes to its business arrangements or the results of its security tests.

- **Childrens' Online Privacy Protection Act ("COPPA"):**[13] COPPA, enacted in 1998, grants parents control over what information is collected online from children under the age of 13 and how that information may be used. Operators of websites directed to children under 13 must include a privacy notice that details the information collected from users; a notice to parents that describes the information that may be collected from children on the website; a verifiable parental consent function; a policy detailing the right to revoke consent and have information deleted. In addition, operators of websites directed to children under

[11] 15 U.S.C. §§ 6801-6809.

[12] Financial institutions include banks, securities firms, insurance companies, and companies providing many other types of financial products and services to consumers, including companies involved in lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts and others.

[13] 15 U.S.C. §§ 6501-6506.

13 are required to protect the confidentiality, security, and integrity of any personal information collected online from children.

- **Health Insurance Portability and Accountability Act ("HIPAA"):**[14] The federal regulations issued under HIPAA protect the privacy of personal health information. The HIPAA Privacy Rule covers health plans,[15] health care providers, and health care clearinghouses.[16] In general, these entities may use and disclose personal health information without special permission from patients only for the purposes of treatment, payment, and health care operations. These entities must also furnish patients a Notice of Privacy Practices that explains how the patient's personal health information may be used and what rights the patient has with respect to his or her personal health information.

- HIPAA, enacted in 1996, protects the privacy of personal health information. HIPAA covers health plans,[17] health care providers, and health care clearinghouses.[18] In general, these entities may only use and disclose personal health information for the purposes of treatment, payment and health care operations without special permission from patients. These entities must furnish patients a Notice of Privacy Practices that explains how the patient's personal health information may be used and what rights the patient has with respect to his or her personal health information.

- **Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act"):**[19] Although the focus of the CAN-SPAM Act is the prevention of unwanted commercial e-mail, it also contains a "Do Not E-mail"

---

[14] 42 U.S.C. §§ 1320d-1320d(8).

[15] Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations, Medicare, Medicaid, Medicare supplement insurers, employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. 45 C.F R. § 160.102, 160.103.

[16] Health care clearinghouses are entities that process information from one entity that is not in a standard format into one that is in a standard format or *vice versa*. These organizations include billing services, repricing companies, community health management information systems, and value-added networks. 45 C.F.R. § 160.103.

[17] Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations, Medicare, Medicaid, Medicare supplement insurers, employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. 45 C.F R. § 160.102, 160.103.

[18] Health care clearinghouses are entities that process information from one entity that is not in a standard format into one that is in a standard format or *vice versa*. These organizations include billing services, repricing companies, community health management information systems, and value-added networks. 45 C.F.R. § 160.103.

[19] 15 U.S.C. §§ 7701-7713.

provision that requires commercial e-mail senders to allow recipients to "opt-out." Companies sending commercial e-mail must provide a return e-mail address or another Internet-based response mechanism that allows a recipient to ask the company not to send future e-mail messages to that e-mail address. These requests must be honored. Any opt-out mechanism offered must be able to process opt-out requests for at least 30 days after transmittal of the commercial e-mail. When a company receives an opt-out request, the law allows 10 business days to stop sending e-mail to the requestor's e-mail address. The original sender cannot help another entity send e-mail to that address, or have another entity send e-mail on the original sender's behalf to that address. Finally, it is illegal to sell or transfer the e-mail addresses of people who choose not to receive e-mail, even in the form of a mailing list, unless the company transfers the addresses so another entity can comply with the law.

FTC ENFORCEMENT OF THE PRIVACY LAWS

For the past several years, the FTC has been at the forefront of privacy enforcement. In fact, this past September the FTC announced that it was reorganizing its Bureau of Consumer Protection to create a new Division of Privacy and Identity Theft.[20] The FTC primarily has focused on violations of stated corporate privacy policies, disclosure of non-secured personal information, and identity theft. It has initiated more than 20 investigations related to consumer privacy since 2000 and has entered into at least 14 consent decrees with companies for alleged violations of the privacy laws. In January 2006, the FTC obtained $10 million in civil penalties, and $5 million in consumer redress against ChoicePoint, the largest civil fine ever obtained by the FTC for a security breach. At the press conference announcing the ChoicePoint settlement, Chairman Deborah Platt Majoras stated that "this penalty tells companies that they must protect sensitive consumer report information. They must guard the front door, that is, their procedures for identifying and verifying customers, as well as guard the back door from hackers and other technological threats. . . [B]ut if they don't then we will step in and we will take action and remind them in the strongest possible way that this is their obligation under the law."[21]

The following summarizes key privacy cases at the FTC:

In re ChoicePoint Inc., File No. 052-3069 (Jan. 26, 2006): ChoicePoint, a data broker and aggregator, agreed to $10 million in civil penalties and $5 million in consumer redress to settle FTC charges that its security and record-handling procedures violated consumers' privacy rights and the Fair Credit Reporting Act ("FCRA"). In addition, the FTC alleged that ChoicePoint violated the FTC Act

[20] The Division of Privacy took over the privacy, Gramm-Leach-Bliley, and FCRA/FACTA responsibilities handled by the Division of Financial Practice, as well as the Identity Theft Project housed in the Division of Planning and payment systems handled by the Division of Marketing Practices. The Associate Director for the new Division of Privacy and Identity Protection is Joel Winston, the former Associate Director of the Division of Financial Practices.

[21] Deborah Platt Majoras, Chairman, Fed. Trade Comm'n, News Conference on Data Security 2 (Jan. 26, 2006).

by making false and misleading statements about its privacy procedures. According to the FTC, ChoicePoint's conduct constituted unfair or deceptive act or practices under the FTC Act. ChoicePoint had publicly acknowledged that the personal financial records of more than 163,000 consumers in its database had been compromised and sold to fraudsters. Specifically, the FTC alleged that ChoicePoint engaged in unfair practice by not employing reasonable procedures to screen prospective subscribers to its service, and turning over sensitive personal data to subscribers whose applications raised obvious concerns, including individuals who lied about their credentials and used commercial mail drops as business addresses. The FTC also charged that ChoicePoint failed to tighten its application approval procedures to monitor subscribers, even after receiving subpoenas from law enforcement authorities alerting it to fraudulent activity dating to 2001. According to the FTC, ChoicePoint violated the FCRA by selling consumer reports to subscribers who did not have a permissible purpose to obtain them, and failing to maintain reasonable procedures to verify subscribers' identities and how they intended to use the information. Finally, the FTC charged that ChoicePoint made false and misleading statements about its privacy policies. In addition to the monetary penalties, ChoicePoint agreed to cease furnishing consumer reports to people without a permissible purpose to receive them and to establish and maintain reasonable procedures to screen and verify people and businesses before furnishing consumer reports. The order also requires ChoicePoint to establish, implement, and maintain a comprehensive information-security program designed to protect the security, confidentiality, and integrity of the personal information it collects from or about consumers, and to obtain audits by an independent third-party security professional every other year for 20 years.

In re DSW Inc., File No. 052-3096 (Dec. 1, 2005): The FTC alleged that DSW Inc. engaged in unfair practices by failing to provide reasonable and appropriate security for sensitive customer data. Specifically, the FTC alleged that DSW (1) created unnecessary risks to sensitive information by storing it in multiple files after it no longer needed it for business purposes; (2) failed to use readily-available security measures to limit access to its network via wireless access points; (3) stored the information in an unencrypted format that was easily accessible with a commonly known user ID and password; (4) failed to sufficiently secure the communications between computers on one in-store network to other in-store or corporate networks; and (5) failed to implement sufficient measures to detect unauthorized access. According to the FTC's complaint, approximately 1.4 million credit and debit cards and 96,000 checking accounts were compromised as a result of DSW's security breaches. As of the time of the Complaint, there were several fraudulent charges on some of the accounts and some customers whose checking account information was compromised were advised to close their accounts, thus incurring out-of-pocket expenses. DSW provided some amount of reimbursement to these customers. DSW agreed to implement a comprehensive information-security program and obtain audits by an independent third-party security professional every other year for 20 years.

In re BJ's Wholesale Club, Inc., File No. 0423160 (June 16, 2005): The FTC alleged that BJ's lax security compromised thousands of credit and debit cards. Specifically, the FTC charged that BJ's did not provide reasonable security for sensitive customer information including (1) failing to encrypt customer information when it was stored on computers in BJ's stores; (2) creating unnecessary risks by storing customer information for up to 30 days in violation of bank security rules, even though it no longer needed the data; (3) storing the information in files that could be accessed using commonly known default user IDs and passwords; (4) failing to use readily-available security measures to prevent unauthorized wireless connections to its networks; and (5) failing to use measures sufficient to detect unauthorized access to the networks or conduct security investigations. According to the FTC's complaint, as a result of these security breaches, fraudulent purchases were made using counterfeit copies of credit and debit cards used at BJ's stores. According to BJ's SEC filings, as of May 2005, claims for these fraudulent purchases totaled approximately $13 million. BJ's agreed to implement a comprehensive information-security program and obtain audits by an independent third-party security professional every other year for 20 years.

In re Petco Animal Supplies, Inc., File No. 032 3211 (Nov. 17, 2004): The FTC alleged security flaws allowed hackers to access consumers' credit card information through its website. Specifically, the FTC charged that Petco failed to implement reasonable and appropriate security measures to secure and protect sensitive customer information, including simple, readily available defenses. The FTC also charged that the sensitive information Petco obtained through its website was not maintained in an encrypted format as the company had claimed. As a result, a hacker was able to penetrate the website and access credit card numbers stored in an unencrypted format. The FTC alleged that Petco's claims were deceptive. The settlement prohibited Petco from misrepresenting the extent to which it maintains and protects sensitive consumer information. It also required that Petco establish and maintain a comprehensive information security program and have a third party conduct biennial audits of its security program for 20 years.

In re Guess?, Inc. and Guess.com, Inc., File No. 022-3260 (June 18, 2003): The FTC alleged that Guess made false claims about information security. Specifically, the FTC charged that the company misrepresented that the personal information it obtained from consumers through its website was stored in an unreadable, encrypted format at all times. The complaint also alleged that Guess misrepresented that it implemented reasonable and appropriate measures to protect personal information. The FTC charged that this claim was false because Guess did not employ appropriate measures to detect vulnerabilities to its system. The settlement prohibits the company from misrepresenting the extent to which it maintains the security of personal information collect from or about consumers. It also requires that Guess establish and maintain a comprehensive information security program. In addition, the settlement requires that Guess hire a third party to conduct biennial audits of its security program.

STATE SECURITY BREACH NOTIFICATION LAWS

In 2005 alone, nearly 20 state legislatures passed consumer security breach notification statutes, many modeled after California's notification law. These laws generally require any business or government agency storing computerized personal data to notify state residents whenever their names, Social Security numbers, driver's license numbers, or financial account data have been accessed by an unauthorized user. California's law initially forced ChoicePoint to disclose that it had been deceived into selling personal consumer information to fraudulent purchasers and led to the FTC's investigation and subsequent settlement for record fines. States are expected to continue being extremely active in this arena.

PRACTICAL ADVICE TO HELP ENSURE COMPLIANCE WITH PRIVACY LAWS

1. Have a Security Incident Response Plan in place before a security breach occurs. This is critical since the question is not if a breach will occur, but when. This is a plan that delineates the steps the company should take before, during, and after any security breach. Below are a few examples of the types of initiatives that a company should consider. Note that a comprehensive Incident Response Plan should include many more components and detail.

    a. Train employees in relevant areas (*e.g.*, IT, customer service, legal) about their roles and responsibilities with regards to the incident, and collect 24/7 contact numbers for an incident response team.

    b. Determine which law enforcement offices are most appropriate to contact in the event of a breach that may involve illegal activities (*e.g.*, Secret Service field office and local police).

    c. Take steps necessary to contain the breach, and conduct a preliminary internal assessment of the scope of the breach.

    d. If your company has determined that it is required to provide notice in certain states, ascertain which individuals must be notified.

    e. Coordinate notification with Credit Reporting Agencies if the breach involves more than 1,000 individuals.

    f. Consider SEC requirements regarding "reportable" events, and whether your company needs to notify the markets prior to or subsequent to notifying the affected individuals.

    g. Consider a public relations and government affairs strategy.

h. Consider whether to offer a credit monitoring service to help affected individuals monitor their credit reports.

2. If your company collects private personal information from consumers, create a privacy policy and follow it to the letter. If your company already has a privacy policy in place, ensure that it is comprehensive and that the company is in full compliance with it.

3. Limit the information your company collects to information that is absolutely necessary to achieve the company's business goals.

4. Secure your data, particularly financial information subject to the provisions of the GLB Act and medical information subject to HIPAA. Keep in mind that this includes not only consumer information, but also employees' personal data. Your company should periodically revisit current security measures, given advances in technology.

5. Ensure that your company's information security program addresses not only electronic information systems, but also all other locations where personal information may be stored, transmitted, or maintained (*e.g.*, laptop computers, back-up tapes, paper files, *etc.*).

6. Take complaints seriously and address them promptly.

7. Educate yourself about state and foreign privacy laws, particularly in the European Union, and ensure compliance with any additional obligations under those laws. If, for example, your company collects any personal information from customers in the EU, it will be subject to significantly more burdensome privacy laws.[22]

8. If your company is consumer-oriented and collects sensitive personally identifiable information, designate a chief privacy officer to oversee compliance with the privacy laws.

9. If your company utilizes e-mail for marketing purposes, ensure that the company is in compliance with the CAN-SPAM Act and any other state laws that address electronic marketing messages.

[22] The EU data privacy directive, EU Directive 95/46/EC, took effect in 1998. The EU privacy laws include the directive itself plus the various laws enacted by EU member nations. The laws dictate the specific ways that personal data may be collected, processed, used, and transferred. Under the laws, the collection and use of personal data must be reasonable given the circumstances. Individuals must also be aware of the data collection, and in some cases must consent to it. In addition, individuals have the ability to object to dissemination of their data to third parties for marketing purposes. The EU laws apply to the collection and processing of employee and HR data; the collection and processing of customer data, even in a business-to-business context; payroll services; data center processing; and the use of vendors for remote housing of personal data and applications.

10. If your company conducts telemarketing, ensure that the company is in compliance with the FTC and FCC Telemarketing Rules. In particular, you need to consistently monitor compliance with the Do Not Call rules, which the FTC enforces vigorously.

11. If your company markets its products to children, ensure that the company is in compliance with COPPA. This is another area of significant FTC enforcement.