SIGNIFICANT DEVELOPMENTS IN
COMPUTER AND CYBERSPACE LAW

CHAPTER 3

Privacy and Compliance – A Coming Out Year

Ronald I. Raether, Jr.
Michael Lamb

CHAPTER 3

SIGNIFICANT DEVELOPMENTS IN COMPUTER AND CYBERSPACE LAW

University of Dayton School of Law

PRIVACY AND COMPLIANCE

"A Coming Out Year"

June 9, 2006

Michael C. Lamb
Vice President and Chief Regulatory Counsel
LexisNexis Risk Management
6601 Park of Commerce Blvd.
Boca Raton, FL 33487
(561) 999-3975
michael.lamb@lexisnexis.com

Ronald I. Raether, Jr.
Faruki Ireland & Cox P.L.L.
500 Courthouse Plaza, S.W.
10 North Ludlow Street
Dayton, OH 45402
(937) 227-3733
rraether@ficlaw.com

MICHAEL C. LAMB

Michael is an experienced technology and information services counsel. A 1981 *summa cum laude* graduate of Boston University School of Law, Michael later held several legal positions at AT&T, including Chief Counsel, AT&T WorldNet Internet Services and Chief Counsel, AT&T Consumer Sales and Marketing. Michael was also the first Chief Privacy Officer at AT&T.

In 2005, Michael joined LexisNexis as Chief Regulatory Counsel and as General Counsel for LexisNexis Risk Management. In these roles, he frequently addresses the application of privacy and information regulations to the array of identity, background and public records services offered by LexisNexis Risk Management.

Michael speaks frequently on privacy matters. He has testified before Congress on telecommunications and cable privacy regulations and has spoken on privacy issues to groups ranging from the Georgetown University Corporate Counsel Institute to the AARP annual convention.

RONALD I. RAETHER, JR.

Ron has handled numerous matters involving technology-related issues. These technology-related matters have spanned numerous legal areas, including antitrust, contracts, employment, trademark, domain name disputes, and federal and state privacy statutes. Ron has authored technology-related articles, such as "Getting Over Y2k Computer Rough Spots: Litigate, Settle or Ignore," Business Law Today, (September/October 2000) and "E-Mail Maelstrom: Electronic Documents Must Be Managed," Business Law Today (September/October 2003). Ron has been a featured speaker on the use of technology in the courtroom and electronic discovery, and has been active in I-Zone (a business designed to assist technology entrepreneurs).

Ron is a member of the Bars of the States of Ohio and Minnesota, the United States District Court for the Southern District of Ohio, and the Court of Appeals for the Sixth, Tenth, and Eleventh Circuits. Ron has been admitted pro hac vice in state and federal courts throughout the United States, including Florida, Louisiana, Missouri, and Utah, and has argued motions or tried cases in many of these jurisdictions. One recent example where Ron successfully argued a motion was reported at 302 F. Supp. 2d 654 (E.D. La. 2004), where the court granted motions to dismiss a putative class action raising federal privacy claims.

Ron resides in Centerville, Ohio with his wife, Marlene, and three daughters. He is a 1996 magna cum laude graduate of the University of Dayton School of Law, where he was an associate editor of the University of Dayton Law Review and where, since 2001, Ron has been an adjunct professor, teaching a trademark trial practice course. He graduated with honors in 1991 from The Ohio State University (B.A. History, Political Science, Economics).

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY

Many have referred to 2005 as the year security data breaches went from being the concern of those involved in security to being discussed in boardrooms, and there are no signs that the increased reports of security data breaches are slowing down in 2006. The protection of personally identifiable information is now the hot button issue as news reports break regarding security data breaches on an almost weekly basis. According to the Privacy Rights Clearinghouse, since the ChoicePoint announcement on February 15, 2005, until May 2006, there have been over 160 announcements regarding security data breaches involving the personally identifiable information of as many as 55 million people. Privacy Rights Clearinghouse, A Chronology of Data Breaches Reported Since the ChoicePoint Incident, at http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited on May 13, 2006). As a result, privacy and compliance issues have moved to the forefront as a concern for citizens whose information is placed at risk, and the businesses, large and small, that collect, store, and disseminate that information.

Against that backdrop, there has been increased pressure for new legislation and regulation to protect personally identifiable information. While the fervor regarding security of personally identifiable information and the need for legislation and regulation has increased, the demand for such protection is not new. In fact, there already exist many federal and state laws that protect personally identifiable information. A brief sampling of some of the more prominent existing federal and state laws are described in Part II. A sampling of some of the pending federal legislation is described in Part III.

In addition to the demand for new legislation and regulation, the last few years have seen a marked increase in government and individual litigation of privacy issues. Part IV provides a summary of some of the recent key cases brought by the Federal Trade Commission regarding the protection of personally identifiable information. Part V provides a summary of some of the more significant civil litigation involving the protection of personally identifiable information in the past few years.

II. EXISTING LAWS REGARDING THE PROTECTION OF PERSONAL INFORMATION

A. FEDERAL LEGISLATION

1. The Privacy Act

The Privacy Act of 1974 limits the collection, use, and disclosure of personal information by the United States government. 5 U.S.C. § 552, et seq. However, the Privacy Act does not address issues relating to data brokers, collection agencies, or consumer credit groups. Id. The purpose of the Privacy Act is to protect citizens against the improper disclosure of personal information about them by government agencies and to delineate the duties and responsibilities of those agencies that collect, store, and disseminate personal information about individuals. Thomas v. U.S. Dep't of Energy, 719 F.2d 342, 346 (10th Cir. 1983).

The Privacy Act provides that a federal agency may collect and store personal information regarding individuals only if the information is "relevant and necessary to accomplish a purpose of the agency." § 552a(e)(1). The Act defines personal information as records relating to "education, financial transactions, medical history, and criminal or employment history [that contains a person's] name, or identifying number, symbol, or other

identifying particular assigned to the individual, such as a finger or voice print or a photograph." § 552a(a)(4).

The Privacy Act prohibits federal agencies from disclosing personal information, unless the disclosure falls within one of the statutory defined exceptions, including individual written consent and a court order. § 552a(b)(1)-(12). In addition, the Act mandates that each federal agency must have in place administrative and physical security systems to prevent the unauthorized release of personal information. § 552a(e)(1)-(12).

2. Driver's Privacy Protection Act

The Driver's Privacy Protection Act of 1994 ("DPPA") limits the use and disclosure of both "personal information" that is "obtained by the [state motor vehicle] department in connection with a motor vehicle record." 18 U.S.C. § 2721(a). "Personal information" is any "information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information." § 2725(3).

The DPPA permits the disclosure of personal information to only certain limited permissible purposes. § 2721(b). The delineated permissible purposes under the DPPA include:

1. Use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.

2. Use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts and dealers; motor vehicle market research activities, including survey research; and removal of non-owner records from the original owner records of motor vehicle manufacturers.

3. Use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only (A) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and (B) if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.

4. Use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.

5. Use in research activities, and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals.

6. Use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.

7. Use in providing notice to the owners of towed or impounded vehicles.

8. Use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection.

9. Use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under Chapter 313 of Title 49 [49 U.S.C. § 31301 et seq.].

10. Use in connection with the operation of private toll transportation facilities.

11. Any other use in response to requests for individual motor vehicle records if the State has obtained the express consent of the person to whom such personal information pertains.

12. Use for bulk distribution for surveys, marketing or solicitations if the State has obtained the express consent of the person to whom such personal information pertains.

13. Use by any requester, if the requester demonstrates it has obtained the written consent of the individual to whom the information pertains.

14. Use for any other use specifically authorized under the law of the State that holds the record, if such use is related to the operation of a motor vehicle or public safety.

§ 2721(b)(1)(14).

The DPPA does permit the resale or re-disclosure of personal information by an authorized recipient for certain limited permissible uses. § 2721(c). While such resale or re-disclosure is permitted, the authorized recipient that resells or re-discloses personal information must maintain records of the disclosure for five years. Id.

The DPPA provides for both criminal and civil penalties for violations. Criminal prosecution requires a "knowing" violation and results in a fine. § 2723(a). Civil penalties may include actual damages, statutory damages, punitive damages, reasonable attorneys' fees and costs, and "other preliminary and equitable relief as the court determines to be appropriate." § 2724(b).

3. Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 ("HIPPA") requires healthcare providers and insurers to create and maintain electronic patient records, or "individually identifiable health information" or protected health information ("PHI"). 42 U.S.C. § 1320d. HIPPA defines PHI as any data "created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse" that relates to a patient's physical or mental condition or care. § 1320d-4.

In an effort to protect PHI data, HIPPA provides that the Department of Health and Human Services may promulgate privacy and security regulations to protect the information. § 1320d-1. The key privacy provisions include:

1. Access for individuals to data and ability to request a correction of errors;

2. Information provided to individuals regarding how their PHI data will be used;

3. PHI cannot be used for marketing purposes without the express consent of the individuals;

4. Information provided to individuals about the reasonable steps used by the provider to ensure that their information remains confidential;

5. Procedures for formal privacy-related complaints to the Department of Health and Human Services Office of Civil Rights;

6. Requirement that providers document privacy policies; and

7. Requirement that providers designate a privacy officer and provide training to employees.

42.C.F.R. §§ 160, 162, and 164 (2006).

To complement HIPPA's privacy provisions, the Department of Health and Human Services also has promulgated certain security regulations that are designed to protect PHI. § 164. The security regulations are divided into three separate segments: administrative; physical; and technical safeguards. § 164.

The administrative safeguards require policies and procedures that are designed to show how the provider will comply with HIPPA. § 164.308. The safeguards include:

1. Requirement that providers adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures;

2. Policies must reference management oversight to ensure compliance with the documented security controls;

3. Procedures should identify employees or classes of employees that have access to PHI (should be limited to only those employees that have a need for the information);

4. Procedures must address access authorization, establishment, modification and termination;

5. Requirement for ongoing training program regarding handling of PHI;

6. Ensure that third parties or vendors handling PHI have sufficient security policies in place;

7. Requirement for the development of contingency plans for emergencies, including disaster recovery procedures;

8. Require internal audits of HIPPA compliance; and

9. Instructions for responding to security breaches.

Id.

The physical safeguards require policies and procedures to protect against inappropriate access to protected data. § 164.310. The safeguards include:

1. Require that provider designate employee to manage and oversee data protection;

2. Require that controls are used for the introduction and removal of hardware and software when PHI is stored on a network;

3. Limit access to equipment (including hardware and software) containing PHI;

4. Require access controls, including facility security plans, maintenance records, and visitor sign-in and escorts;

5. Policies addressing proper workstation use, including policies to protect against public viewing PHI; and

6. Policies requiring providers to utilize contractors or agents that are fully trained on protecting PHI.

Id.

The technical safeguards require policies and procedures to control access to computer systems that contain or transmit PHI. § 164.312. The safeguards include:

1. Requirement that information systems that contain PHI are protected from intrusion through the use of encryption (open networks) or access controls (closed systems/networks);

2. Policies that ensure that PHI in systems is not changed or erased in an unauthorized manner;

3. Requirement that computer systems use a form of data corroboration to ensure data integrity;

4. Requirement that providers use security authentication protocols such as password systems, two- or three-way handshakes, telephone callbacks, or token systems;

5. Requirement that providers make documentation of policies available to government;

6. Requirement that information security policies provide written record of all configuration settings on the components of the networks; and

7. Requirement that providers have documented risk analysis and risk management programs.

Id.

HIPPA imposes civil and criminal penalties on persons who improperly handle or disclose PHI. § 1320d.

4. Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act or Financial Services Modernization Act of 1999 ("GLBA") regulates the collection, use, and disclosure of a consumer's financial information by "financial institutions" (e.g., non-bank mortgage lenders, loan brokers, and some financial or investment advisers). 15 U.S.C. § 6801. Generally, the GLBA governs the collection, disclosure, and protection of consumers' nonpublic person information or personally identifiable information by financial institutions. § 6801, et seq., and § 6821, et seq. The major components regarding privacy protections in the GLBA include the Financial Privacy Rule and the Safeguard Rule, which where promulgated by the Federal Trade Commission.

The Financial Privacy Rule requires financial institutions to provide each consumer with a privacy notice upon the establishment of the consumer relationship and then each subsequent year. 16 C.F.R. § 313. Generally, the privacy notice must explain the

information collected about the consumer, where that information is stored, how that information is used, and how that information is protected. Id. The notice also must identify the consumer's right to opt-out of the information being shared with unaffiliated parties. Id.

The Safeguard Rule requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect consumers' nonpublic personal information. 16 C.F.R. § 314. Generally, the plan must include: (1) a designation of an employee to manage the safeguards; (2) a review of the risk management of each department handling the nonpublic personal information; (3) a plan for developing, monitoring, and testing a program to secure information; and (4) a plan for changing the safeguards as needed. Id.

B. STATE LEGISLATION

1. California's Senate Bill 1386

In 2002, California became the first state to enact legislation directed toward notification after a security data breach. Cal. Civ. Code § 1798.29 (2006). The California law, commonly known as Senate Bill 1386, requires companies that store personal information data electronically to notify California consumers of a security breach if the company knows or reasonably believes that unencrypted information about the consumer has been subject to a security data breach. Id.

Senate Bill 1386 has been referred to as one of the most significant privacy laws to have been enacted in years as the California law requires companies to provide consumers with advance notice when their personal information may have been subject to an unauthorized access. It is this law that is credited with requiring the security breach notifications that were

provided after the ChoicePoint incident (discussed below). After the reported security data breaches in 2005, many states have enacted statutes similar to California's Senate Bill 1386 that require notification to persons after security data breaches.

2. Chart of State Notification Statutes

At least 24 states have enacted statutes that require notification to a person whose personal information (electronically stored) was accessed by another person or business without authorization. Many of these statutes are based, in large part, on California's Senate Bill 1386 (discussed above). The key provisions of the state statutes are summarized in the chart below.

The "Protected Information" column below provides a summary of the information that is protected under the statute. Many states provide for exceptions to the notification requirement in certain circumstances. The "Encryption Exception" column below identifies the states that provide an exception that does not require notification when the data that was subject to the security breach was encrypted. The "Publicly Available Exception" column below identified the states that do not require notification if the personal information was gathered from a publicly available source. The "Delay" column below provides a summary of the states that allow a company to delay the sending of the notification to allow law enforcement a reasonable amount of time to conduct an investigation. The "Enforcement" column identifies the enforcement authority under each statute and whether the statute expressly permits private causes of actions.

STATE	EFFECTIVE DATE	PROTECTED INFORMATION	ENCRYPTION EXCEPTION	PUBLICLY AVAILABLE EXCEPTION	DELAY	ENFORCEMENT
Arkansas	August 12, 2005	(1) Social Security Number; (2) Driver's License Number or Arkansas ID number; (3) Account number in combination with security code or password; and (4) Medical Information.	√		√	Attorney General Enforcement
California	July 1, 2003	(1) Social Security Number; (2) Driver's License Number or California ID number; and (3) Account number in combination with security code or password.	√	√	√	Attorney General Enforcement Private Cause of Action
Connecticut	January 1, 2006	(1) Social Security Number; (2) Driver's License Number or Connecticut ID number; and (3) Account number in combination with security code or password.	√	√	√	Attorney General Enforcement

STATE	EFFECTIVE DATE	PROTECTED INFORMATION	ENCRYPTION EXCEPTION	PUBLICLY AVAILABLE EXCEPTION	DELAY	ENFORCEMENT
Delaware	June 28, 2005	(1) Social Security Number; (2) Driver's License Number or Delaware ID number; and (3) Account number in combination with security code or password.	√	√	√	Attorney General Enforcement
Florida	July 1, 2005	(1) Social Security Number; (2) Driver's License Number or Florida ID number; and (3) Account number in combination with security code or password.	√	√	√	Attorney General Enforcement
Georgia	May 5, 2005	(1) Social Security Number; (2) Driver's License Number or Georgia ID number; (3) Account number; and (4) Passwords or access codes.	√	√	√	

STATE	EFFECTIVE DATE	PROTECTED INFORMATION	ENCRYPTION EXCEPTION	PUBLICLY AVAILABLE EXCEPTION	DELAY	ENFORCEMENT
Illinois	January 1, 2006	(1) Social Security Number; (2) Driver's License Number or Illinois ID number; and (3) Account number.	√	√		Attorney General Enforcement Private Cause of Action
Indiana	July 1, 2006	(1) Social Security Number; (2) Driver's License Number or Indiana ID number; and (3) Account number with security code, access code, or password.	√	√	√	Attorney General Enforcement
Louisiana	January 1, 2006	(1) Social Security Number; (2) Driver's License Number or Louisiana ID number; and (3) Account number with security code or password.	√	√	√	Attorney General Enforcement

STATE	EFFECTIVE DATE	PROTECTED INFORMATION	ENCRYPTION EXCEPTION	PUBLICLY AVAILABLE EXCEPTION	DELAY	ENFORCEMENT
Maine	January 31, 2006	(1) Social Security Number; (2) Driver's License Number or Maine ID number; and (3) Account number with security code or password.	√	√	√	Attorney General Enforcement
Minnesota	January 1, 2006	(1) Social Security Number; (2) Driver's License Number or Minnesota ID number; and (3) Account number with security code or password.	√	√	√	Attorney General Enforcement Private Cause of Action
Montana	March 1, 2006	(1) Social Security Number; (2) Driver's License Number or Montana ID number; and (3) Account number with security code or password.	√	√	√	Department of Administration Enforcement

STATE	EFFECTIVE DATE	PROTECTED INFORMATION	ENCRYPTION EXCEPTION	PUBLICLY AVAILABLE EXCEPTION	DELAY	ENFORCEMENT
Nevada	January 1, 2006	(1) Social Security Number or employer identification number; (2) Driver's License Number or Nevada ID number; and (3) Account number with security code or password.	√	√	√	Attorney General Enforcement County District Attorney Enforcement
New Jersey	January 1, 2006	(1) Social Security Number; (2) Driver's License Number or New Jersey ID number; (3) Account number with security code or password; and (4) Disassociated data that links to personal information.	√	√	√	Attorney General Enforcement Private Cause of Action
New York	December 7, 2005	(1) Social Security Number; (2) Driver's License Number or New York ID number; and (3) Account number with security code or password.	√	√	√	Attorney General Enforcement

STATE	EFFECTIVE DATE	PROTECTED INFORMATION	ENCRYPTION EXCEPTION	PUBLICLY AVAILABLE EXCEPTION	DELAY	ENFORCEMENT
North Carolina	December 1, 2005	(1) Social Security Number or Employer Taxpayer Identification Number; (2) Driver's License Number or Passport Number; (3) Account Number; (4) PIN Code; (5) Digital Signature; (6) Information that permits access to financial resources; (7) Biometric Data; and (8) Fingerprints.	√	√	√	Attorney General Enforcement Private Cause of Action

STATE	EFFECTIVE DATE	PROTECTED INFORMATION	ENCRYPTION EXCEPTION	PUBLICLY AVAILABLE EXCEPTION	DELAY	ENFORCEMENT
North Dakota	June 1, 2005	(1) Social Security Number; (2) Driver's License Number or North Dakota ID number; (3) Account number with security code or password; (4) Date of Birth; (5) Mother's Maiden Name; (6) Employer Identification Number; and (7) Digitized or Electronic Signature.	√	√	√	Attorney General Enforcement
Ohio	February 17, 2006	(1) Social Security Number; (2) Driver's License Number or Ohio ID number; and (3) Account number with security code, access code, or password.	√	√	√	Attorney General Enforcement

STATE	EFFECTIVE DATE	PROTECTED INFORMATION	ENCRYPTION EXCEPTION	PUBLICLY AVAILABLE EXCEPTION	DELAY	ENFORCEMENT
Pennsylvania	June 20, 2006	(1) Social Security Number; (2) Driver's License Number or Pennsylvania ID number; and (3) Account number with security code, access code, or password.	√	√	√	Attorney General Enforcement
Rhode Island	March 1, 2006	(1) Social Security Number; (2) Driver's License Number or Rhode Island ID number; and (3) Account number with security code, access code, or password.	√		√	Attorney General Enforcement
Tennessee	July 1, 2005	(1) Social Security Number; (2) Driver's License Number; and (3) Account number with security code, access code, or password.	√	√	√	Attorney General Enforcement Private Cause of Action

STATE	EFFECTIVE DATE	PROTECTED INFORMATION	ENCRYPTION EXCEPTION	PUBLICLY AVAILABLE EXCEPTION	DELAY	ENFORCEMENT
Texas	September 1, 2005	(1) Social Security Number; (2) Driver's License Number or government issued identification number; and (3) Account number with security code, access code, or password.	√	√	√	Attorney General Enforcement
Utah	January 1, 2007	(1) Social Security Number; (2) Account number with security code, access code, or password; and (3) Driver's License Number or Utah ID number.	√		√	Attorney General Enforcement
Washington	July 24, 2005	(1) Social Security Number; (2) Driver's License Number or Washington ID number; and (3) Account number with security code, access code, or password.	√	√	√	Attorney General Enforcement Private Cause of Action

STATE	EFFECTIVE DATE	PROTECTED INFORMATION	ENCRYPTION EXCEPTION	PUBLICLY AVAILABLE EXCEPTION	DELAY	ENFORCEMENT
Wisconsin	March 31, 2006	(1) Social Security Number; (2) Driver's License Number or Wisconsin ID number; (3) Account number with security code, access code, or password; (4) DNA; and (5) Biometric Data, including fingerprint, voice print, retina or iris image, or any other unique characteristic.		√	√	

3. "Baby" Driver's Privacy Protection Acts

At least 35 states have passed statutes similar to the federal DPPA. E.g., Ohio Rev. Code § 4501.27; Tex. Transp. Code § 730.001, et seq. Eleven of these states follow the record-keeping procedures set forth in 18 U.S.C. § 2721(c).

4. "Little" FTCAs

Each state (and the District of Columbia) has enacted statutes that prohibit "unfair methods of competition," "unfair or deceptive acts or practices," "unconscionable" acts, and/or false or misleading practices. E.g., Cal. Bus. & Prof. Code § 17200, et seq.; N.Y. Gen. Bus. Law § 349, et seq.; Ohio Rev. Code §§ 1345.01, et seq., 4165.01, et seq. According to the express statutory language or relevant caselaw, roughly one-half of the "little" FTCAs (the Federal Trade

Commission Act or "FTCA" is discussed in section IV below) are construed by following, or giving great weight to, Section 5 of the FTCA or by using Section 5 as a guide.

III. SAMPLING OF PENDING LEGISLATION REGARDING THE PROTECTION OF PERSONAL INFORMATION

There are a number of different bills currently pending in the Senate and House of Representatives regarding the protection of personal information. Below is a summary of some of those pending bills.

A. SOCIAL SECURITY NUMBER MISUSE PREVENTION ACT (Senate Bill No. 29)

The Social Security Number Misuse Prevention Act seeks to prohibit the display, sale, or purchase of social security numbers by the government or private businesses without the express consent of the individual, except in specified circumstances. It provides for civil and criminal penalties and private causes of action. This Bill was introduced by Senator Diana Feinstein on January 24, 2005 and is currently pending in the Committee on the Judiciary.

B. SOCIAL SECURITY NUMBER PRIVACY AND IDENTITY THEFT PREVENTION ACT (House of Representatives Bill No. 1745)

The Social Security Number Privacy and Identity Theft Prevention Act seeks to prohibit the display of social security numbers on all government issued checks and identification cards. In addition, the Bill bans the sale, purchase and display of social security numbers and using a social security number to locate or identify individuals with intent to injure or use their identification for any illegal purpose. The Bill also makes a refusal to do business without receipt of social security number an unfair or deceptive act or practice. The Bill establishes civil and criminal penalties, and enhanced penalties in case of terrorism, drug

trafficking, violence, or prior offenses. The Bill was introduced on April 20, 2005 by Representative Clay Shaw Jr. and is currently pending in the House Subcommittee on Financial Institutions and Consumer Credit.

C. PERSONAL DATA PRIVACY AND SECURITY ACT
(Senate Bill No. 1332)

The Personal Data Privacy and Security Act of 2005 seeks to grant individuals the right to access and establish procedures for correcting information collected by data brokers. The Bill also requires businesses that collect personally identifiable information to develop and publish a data privacy and security program. In addition, the Bill enhances criminal penalties for ID theft, and appropriates $25 million a year for grants to state and local governments for enforcement purposes.

The Bill also would require notification to individuals affected by a security breach and establishes fines and terms of imprisonment for concealment. However, the Bill provides exemptions for entities that perform a risk assessment that concludes that there was, or will not be, any harm to individuals affected, or that participate in a security program designed to block the use of personal information for unauthorized financial transactions before they are charged to an individual's account. The terms of the Bill require the evaluation and audit of security and privacy policies of government contractors. This Bill was introduced by Senator Arlen Specter on June 29, 2005 and has been referred to the Senate Committee on the Judiciary.

D. CONSUMER DATA SECURITY AND NOTIFICATION ACT
(House of Representatives Bill No. 3140)

The Consumer Data Security and Notification Act would make the information collected by data brokers subject to many of the provisions covering consumer reports under the

Fair Credit Reporting Act. The Bill directs the Federal Trade Commission to establish security, confidentiality, and notification regulations for consumer reporting agencies. The Bill amends the Gramm-Leach-Bliley Act to require financial institutions to notify customers of security breaches. The Bill was introduced by Representative Melissa Bean on June 30, 2005 and has been referred to the House Committee on Financial Services.

E. INFORMATION PROTECTION AND SECURITY ACT
(Senate Bill No. 500)

The Information Protection and Security Act would direct the Federal Trade Commission to regulate information brokers. Under the Bill, data brokers are required to ensure data accuracy and confidentiality, authenticate and track users, detect and prevent unauthorized activity, and mitigate potential harm to individuals. In addition, the Bill provides an individual a right to access, correct, and know which third parties have procured their personal information. Any violations of the regulation are unfair or deceptive acts of practices under the Federal Trade Commission Act. In addition, the Bill provides individuals with a private right of action if injured by a violation. The Bill also allows states the ability to bring civil actions on behalf of residents. The Bill was introduced by Senator Bill Nelson on March 3, 2005 and is currently before the Senate Committee on Commerce, Science, and Transportation

F. COMPREHENSIVE IDENTITY THEFT PREVENTION ACT
(Senate Bill No. 768)

The Comprehensive Identity Theft Prevention Act would provide for limits on the sale of personally identifiable information. In addition, the Bill creates notification requirements in case of unauthorized acquisition of sensitive personal information. With certain exceptions, the Bill prohibits the solicitation, sale, purchase, use, and access to social security numbers. The Bill also establishes the Office of Identity Theft within the Federal Trade Commission for

enforcement. The Bill was introduced by Senator Charles Schumer on April 12, 2005 and has been referred to the Senate Committee on Commerce, Science, and Transportation.

G. IDENTITY THEFT PROTECTION ACT (Senate Bill No. 1408)

The Identity Theft Protection Act would direct the Federal Trade Commission to promulgate regulations that require certain businesses to develop and implement information security programs to protect personal information. The Bill requires the businesses to provide notification of a security breach that affects more than 1,000 individuals. In addition, the Bill prohibits businesses from soliciting social security numbers, unless there is a specific use for which no other identifier can reasonably be used. The Bill also allows state attorney generals to bring civil actions on behalf of its residents for violations. The Bill was introduced by Senator Gordon Smith on July 14, 2005 and is currently pending in the Senate Committee on Commerce, Science, and Transportation.

IV. RECENT ACTIONS BROUGHT BY THE FEDERAL TRADE COMMISSION REGARDING THE PROTECTION OF PERSONAL INFORMATION

Although not specifically written as a privacy law, the Federal Trade Commission has been using the Federal Trade Commission Act ("FTCA") to regulate and protect personal information. Section 5 of the FTCA provide the Federal Trade Commission with enforcement authority over "unfair or deceptive acts or practices." 15 U.S.C. Sec. 45(a)(1).

The FTC enforces the substantive requirements of Section 5 through both administrative and judicial processes. In the administrative process, the FTC makes the initial determination whether the practice is an unfair or deceptive trade practice. When the FTC determines that there is reason to believe that an unfair or deceptive trade practice has occurred,

the FTC may issue a complaint setting forth its charges. Faced with a complaint, a party may elect to sign a consent agreement without admitting liability.

Below are brief summaries of some of the recent enforcement actions and settlements regarding privacy issues and the protection of personal information that have been brought by the Federal Trade Commission through the use of the unfair methods of competition and unfair or deceptive acts or practices provisions of Section 5 of the FTCA.

A. "DECEPTIVE ACTS OR PRACTICES" ENFORCEMENT ACTIONS

1. In the Matter of Eli Lilly & Company

In early 2002, the Federal Trade Commission reached a settlement with Eli Lilly & Company, which had inadvertently disclosed the email addresses of 669 of the subscribers to its Prozac mailing list. The disclosure was contrary to the company's privacy statement as the statement promised that the information that was submitted by customers would not be disclosed and that the company had security measures in place to maintain the privacy of information.

As part of the settlement, the Eli Lilly & Company agreed to refrain from misrepresenting the extent to which privacy, confidentiality, or security of customers' data is protected, to implement a written security program for the collection of personally identifiable information, and to retain documents for five years to show compliance with the order.

2. In the Matter of Microsoft Corporation

In 2002, the Federal Trade Commission reached a settlement with Microsoft after the company made various representations regarding purchases made by Microsoft's Passport Wallet system and privacy on its website. The Federal Trade Commission found the statements to be deceptive as purchases made with the Passport Wallet were no safer than purchases made

without it. In addition, the Commission found that children could easily access and change the settings after the parent initially set up the perimeters of what the child could submit. The Federal Trade Commission also found that Microsoft obtained and stored, for a limited period of time, a listing of all sites the visitor had been on, which was not disclosed in Microsoft's privacy policy.

Under the terms of the settlement, Microsoft agreed to refrain from misrepresenting information security practices, implement a written security program for the collection of personally identifiable information, and obtain independent assessments from third parties that certify that Microsoft is maintaining sufficient security measures to reasonably ensure that non-public personal information is protected.

3. In the Matter of Guess Jeans, Inc.

In the summer of 2003, the Federal Trade Commission reached a settlement with Guess Jeans, Inc. after the company's representations on the company's websites that information submitted by consumers who made on-line purchases were protected, including that credit card numbers were stored and encrypted in unreadable formats at all times. The Federal Trade Commission found that Guess' databases were vulnerable to commonly known or reasonably foreseeable hacking attacks, which could be used to gain access in clear text to credit card numbers.

As part of the settlement, Guess agreed to refrain from misrepresenting information security practices, implement a written security program for the collection of personally identifiable information, and obtain an independent assessment from third parties

certifying that Guess is maintaining sufficient security measures to reasonably ensure that non-public personal information is protected.

4. In the Matter of Tower Records

In 2004, the Federal Trade Commission reached a settlement with Tower Records after the FTC raised issues regarding the accuracy of representations on the company's website that all of the information collected from consumers who made on-line purchases was safeguarded and that Tower Records would not share personal information with anyone without the express written consent of the consumer. The Federal Trade Commission found that a consumer's order status application on Tower Records' website contained no authentication code to ensure that the consumer accessing the information was the consumer to whom the information pertained. Thus, the vulnerability allowed anyone with a valid order number to access the personal information of other consumers. According to the Federal Trade Commission, the vulnerability was commonly known and reasonably foreseeable.

Under the terms of the settlement, Tower Records agreed to refrain from misrepresenting information security practices, implement a written security program for the collection of personally identifiable information, and obtain an independent assessment from third parties certifying that Tower Records is maintaining sufficient security measures to reasonably ensure that non-public personal information is protected.

5. In the Matter of PETCO Animal Supplies Inc.

In early 2005, the Federal Trade Commission reached a settlement with PETCO Animal Supplies Inc. after it was found that PETCO's website had vulnerabilities that were similar to the vulnerabilities identified in the Guess Jeans' matter. The Commission found that a

hacker could access PETCO's consumer records, including the credit card numbers of its customers. The Federal Trade Commission found that PETCO created these vulnerabilities by failing to implement reasonable security measures to secure and protect sensitive consumer information. In addition, the Commission found that PETCO's customer information was not maintained in an encrypted format.

Under the terms of the settlement, PETCO agreed to refrain from misrepresenting the extent to which it maintained and protected sensitive consumer information, establish and maintain a comprehensive information security program designed to protect the confidentiality and integrity of personal information, and arrange bi-annual audits of its security program by an independent third party.

6. In the Matter of Nations Title Agency, Inc.

In May 2006, the Federal Trade Commission announced that it reached a settlement with Nations Title Agency, Inc. The settlement was reached after the Federal Trade Commission found that National Title failed to provide appropriate security for personal information. The settlement was announced after an investigation was launched following a report in February 2005 that a television station found documents containing personal information in National Title's dumpster in violation of FACTA and GLBA. Like the Safeguard Rule and Privacy Rule of the GLBA, the FTC has also promulgated data security regulations as part of the Fair and Accurate Credit Transaction Act or FACTA. One such rule, the Disposal Rule, requires companies that possess consumer or employee information to properly dispose of the information. In addition, the Commission found that, in April 2004, a hacker used a common website to attack and obtain information from National Title's computer network.

As part of the settlement, National Title agreed to implement a security program to protect personal information, obtain initial and biennial assessments from an independent third party, maintain documents for five years concerning National Title's compliance with the order, and provide proper instructions to all future employees.

B. "UNFAIR METHODS OF COMPETITION" ENFORCEMENT ACTIONS

1. In the Matter of B.J.'s Wholesale Club, Inc.

In June 2005, the Federal Trade Commission announced a settlement with B.J.'s Wholesale Club, Inc. Under the terms of the settlement, B.J.'s agreed to implement a written security program for the collection of personally identifiable information and obtain an independent assessment from a third party certifying that B.J.'s is maintaining sufficient security measures.

The Federal Trade Commission found that B.J.'s failed to maintain reasonable standards to safeguard information obtained from customers when they paid for purchases at B.J.'s retail stores using their credit or debit cards. The Commission also found that B.J.'s failed to encrypt the information, stored the information in files that could be accessed anonymously, and kept the information longer than necessary.

Unlike the cases involving alleged deceptive practices, B.J.'s did not have a written privacy policy that made assurances of a certain level of data protection when collecting consumer data. Instead, the FTC looked at B.J.'s security procedures and procedures, deemed then to be insufficient, and charged B.J.'s with engaging in conduct unfair to consumers. In other words, the FTC signaled to companies that the Commission was making protecting consumers' privacy rights a top priority for the agency. The settlement put companies on notice that the

failure to employee reasonable procedures could result in an unfairness action under Section 5 of the FTCA.

2. In the Matter of DSW, Inc.

In December 2005, the Federal Trade Commission announced that it reached a settlement with DSW, Inc. The settlement stemmed from DSW's March 2005 announcement that a security breach resulted in the potential release of over 100,000 individuals' personal information. The Federal Trade Commission found that DSW created unnecessary risks to stored personal information by failing to employ sufficient measures to detect unauthorized access. In addition, the Commission found that DSW retained personal information in multiple files and stored the information in an unencrypted format, which could be easily accessed by using a commonly known user ID and password. The Commission also found that DSW did not use readily available security measures to limit access to its computer network through wireless access points on the network, and it did not sufficiently limit the ability of computers on one in-store network to connect to computers in other in-store and corporate networks.

Under the terms of the settlement, DSW agreed to establish and implement a comprehensive information security program to protect the security, confidentiality, and integrity of personal information. DSW also agreed to obtain initial and bi-annual assessments from a qualified objective independent third party professional of its security program. In addition, DSW agreed to maintain a copy of each document relating to compliance and make these documents available to the Federal Trade Commission upon request. For a period of ten years, DSW agreed to deliver a copy of the settlement and order to all current and future employees having responsibilities with respect to the subject matter of the order. DSW also agreed to notify the Federal Trade Commission at least 30 days prior to any change in the corporation that could

affect its compliance obligations arising under the order. Finally, DSW agreed that, within 180 days from the approval of the settlement, it would submit a report to the Federal Trade Commission that sets forth in detail the manner and form in which DSW complied with terms of the settlement.

3. United States v. ChoicePoint, Inc.

After ChoicePoint announced that on February 15, 2005 that approximately 145,000 people had their personal information potentially compromised after identity thieves established accounts, the Federal Trade Commission launched an investigation into ChoicePoint's privacy, verification, and compliance practices. The Federal Trade Commission found that ChoicePoint failed to verify properly customers before providing those customers access to consumers' personal information. In addition, the Commission found that ChoicePoint failed to monitor or otherwise identify unauthorized activity, even after it was notified by law enforcement of fraudulent activity between 2001 and 2004 and despite its knowledge of suspicious activity. Additionally, the Commission stated that ChoicePoint made false and misleading representations to both customers and the public about the safeguards employed to protect the security of information and ensure compliance with the FCRA.

On January 26, 2006, the Commission announced a settlement where ChoicePoint agreed to pay a $10,000,000 fine for violations of the Fair Credit Reporting Act ("FCRA") and pay an additional $5,000,000 into a fund for potential consumer redress. The fine was the largest ever levied by the Federal Trade Commission. In addition, as part of the settlement, ChoicePoint agreed, among other things, to: (1) provide FCRA data only to persons with permissible purposes; (2) implement a written security program for the collection of personally identifiable information; and (3) obtain an independent assessment from a third party certifying that it is

maintaining sufficient security measures to reasonably ensure that personal information is protected. Finally, under the terms of the settlement, the Federal Trade Commission retained the right to monitor compliance, including using representatives posing as consumers without prior notice.

4. In the Matter of CardSystems Solutions, Inc.

In February 2006, the Federal Trade Commission announced a settlement with CardSystems Solutions, Inc., which had earlier announced that roughly 40 million accounts could have been vulnerable to an unauthorized access as they retained data from the magnetic strips of credit and debit cards and held that data without adequate security measures. The CardSystems breach reportedly resulted in more than 260,000 cases of identity fraud. After the breach, several major credit card companies (including Visa and American Express) announced that they would no longer allow CardSystems to process transactions made with their cards

As part of the settlement, CardSystems agreed to establish and maintain a comprehensive information security program and obtain, every two years for the next 20 years, an audit from an independent third party professional that confirms that CardSystems' security program meets the standards of the order.

V. RECENT CASES REGARDING THE PROTECTION OF PERSONAL INFORMATION

A. SCOPE OF LIABILITY

1. Russell v. ChoicePoint Servs. et al.

In Russell v. ChoicePoint Servs. et al., 302 F. Supp. 2d 654 (E.D. La. 2003), plaintiffs alleged that defendants (ChoicePoint Services Inc. and Reed Elsevier Inc.) had obtained improperly personal information from motor vehicle records with intent to redistribute

it for an impermissible purpose. Id. at 654. Reed Elsevier moved to dismiss plaintiffs' complaint arguing that (1) plaintiffs lack standing as to the DPPA claims and (2) plaintiffs may not maintain a DPPA claim for improper obtainment without alleging an accompanying improper use. Id. at 663-64.

Reed Elsevier argued that it permissibly obtained plaintiffs' personal information under a DPPA as "[t]he plain language of the DPPA permits entities like Reed Elsevier to obtain driver's personal information from DMVs and subsequently resell that information to third parties with a permissible use." Id. at 664. Agreeing with Reed Elsevier, the court dismissed with prejudice plaintiffs' obtainment DPPA claims, stating that the "obtainment of plaintiffs' personal DMV records for the sole purpose of resale and redisclosure does not entitle plaintiff[s] to relief under the DPPA." Id. at 670.

2. Parus v. Allstate Insurance Company, et al.

In Parus v. Allstate Insurance Company, et al., 2005 U.S. Dist. LEXIS 20183 (September 14, 2005), plaintiff brought an action against the Town of Woodruff, Wisconsin, claiming that the Town illegally obtained his personal information from the Department of Motor Vehicle's database in violation of the DPPA. Id. at *1. Defendants moved for summary judgment claiming, among other things, that plaintiff had not shown that he was injured as a result of the "technical violation of the Act." Id. at *10-11. The court distinguished Russell v. Choicepoint stating that Russell involved "commercial entities" that were permitted to resell the information under the DPPA and, denying the motion for summary judgment, held that "improperly obtaining plaintiff's information *was* an injury." Id. at *12 (emphasis in original).

3. Harrington v. ChoicePoint Inc.

In Harrington v. ChoicePoint Inc., No. CV 05-1294 (C.D. Cal. September 15, 2006), plaintiffs brought a class action against ChoicePoint alleging that the company improperly disclosed information about plaintiffs in violation of the FCRA, CCRAA, ICRAA, California Civil Code § 1785.1 ("Invasion of Privacy"), California Civil Code § 1798.81.5 ("Failure to Maintain Reasonable Security Procedures"), and California Business & Professions Code § 17200. Id. at 2. Plaintiffs based the complaint upon ChoicePoint's announcement, in February 2005 and the subsequent notifications to consumers, that persons had fraudulently posed as legitimate businesses to open accounts as ChoicePoint customers and may have had unauthorized access to their personal information. Id.

ChoicePoint moved for summary judgment on the FCRA claims; asserting that the named plaintiffs did not have their personal information disclosed to the fraudulent customers. Id. at 6. The court denied ChoicePoint's motion for summary judgment and stated that the company failed to proffer sufficient evidence to support its allegation that plaintiffs' information had not been communicated to fraudulent users. Id. at 8. The case remains pending in the United States District Court for the Central District of California.

4. Witriol v. LexisNexis Group, et al.

In Witriol v. LexisNexis Group et al., 2006 U.S. Dist. LEXIS 26670 (Feb. 10, 2006), plaintiff brought a class action against defendants alleging that defendants disclosed consumer reports and personal information about plaintiff (and the proposed class members) without their consent or authorization to third parties who lacked any permissible purpose for receiving and using such information. Id. at *1-2. Plaintiff asserted claims for negligence and

violations of the FCRA, California Credit Reporting Agencies Act ("CCRAA"), and California Investigative Consumer Reporting Agencies Act ("CICRAA"). Id. at *2.

Defendants moved to dismiss the complaint arguing, among other things, that the federal FCRA, CCRAA, and CICRAA are violated by impermissibly "furnishing" a consumer report and, since criminal trespassers obtained the information, defendants assert that they cannot be held liable under the statutes. Id. Plaintiffs argued that dismissing was improper because the motion to dismiss relied on extrinsic evidence and the court agreed in denying the motion. Id.

5. American Bankers Ass'n v. Lockyer

In American Bankers Ass'n v. Lockyer, 2005 U.S. Dist. LEXIS 22437 (E.D. Cal. Oct. 4, 2005), plaintiff asserted an action against several California state officials, claiming that federal statutes (the GLBA and FCRA) pre-empted the sharing provisions of the California Financial Information Privacy Act. Id. at *2. Plaintiffs sought a order from the court declaring that it was legal for affiliated entities to share FCRA regulated personal information. Id. Granting plaintiffs both injunctive and declaratory relief, the court declared that the FCRA's affiliate sharing pre-emption clause pre-empted California law insofar as it attempted to regulate the communication between affiliates of information. Id.

B. DAMAGES

1. Forbes v. Wells Fargo

In Forbes v. Wells Fargo, 420 F. Supp. 2d 1018 (D. Minn. Mar. 16, 2006), plaintiffs-customers filed suit in Minnesota state court, alleging breach of contract, breach of fiduciary duty and negligence, after Wells Fargo allegedly used a service provider to print monthly statements for defendant's customers, and the customer information was stolen from the

server provider's computers. Id. at 1018. The information was unencrypted and included personal information, such as the names, addresses, social security numbers, and account numbers of customers. Id.

Defendant removed the case to federal court and moved for summary judgment. Id. The United States District Court for the District of Minnesota recently granted defendant's motion for summary judgment. Id. Defendants argued that plaintiffs have not suffered any cognizable damage, as there was no indication that the information on the stolen computers had been accessed or misused. Id. The court held that plaintiffs could not maintain a claim without establishing that the persons that were subject to the unauthorized access suffered some cognizable damage. Id.

2. Kehoe v. Fidelity Federal Bank & Trust

In Kehoe v. Fidelity Federal Bank & Trust, 421 F.3d 1209 (2005), Fidelity purchased from the State of Florida's Department of Highway Safety and Motor Vehicles the names and addresses of individuals who had registered new motor vehicles or used motor vehicles less than three years old within the preceding month in certain Florida counties. Id. at 1210-11. The Florida DMV forwarded the information, at Fidelity's request, to a third-party mass mailing service provider, which mailed solicitations to individuals to refinance their motor vehicle loans. Id. at 1211.

Plaintiff brought a class action alleging violations of the DPPA and seeking liquidated damages "in the amount of $2,500.00 for each instance in which [Fidelity] obtained or used personal information concerning [Kehoe] and members of the Class," punitive damages, attorneys' fees and costs, and an injunction ordering the destruction of the information. Id.

Fidelity moved for summary judgment, which was granted by the district court. Id. The district court dismissed plaintiff's claims because plaintiff had failed to prove some measure of actual damages. Id. The Eleventh Circuit Court of Appeals reversed the district court and held that plaintiff need not prove actual damages to recover liquidated damages. Id. at 1217.

169788.1