
INFORMATION SECURITY ISSUES:**UNDERSTANDING THE MODERN INFORMATION SECURITY LAWS****AND IMPLEMENTING INFORMATION SECURITY WITHIN THE ENTERPRISE**

Francoise Gilbert¹
Attorney At Law

INTRODUCTION

Personal information databases have become a critical asset for most organizations, essential for record keeping, customer relations, product support, and other core functions. Typically, these databases include personal details about employees, clients, or prospects such as home addresses, unlisted phone numbers, family status, children's or dependents' names, race, ethnicity or national origin, employment history, salary, or medical information. The information collected might extend to hobbies, personal interests, travels, or membership in community or business organizations. In some cases, this information might be highly sensitive; for example, social security numbers, bank account or credit card numbers, or information about a person's political opinion or sexual orientation.

Given the strategic and monetary value of these compilations, they have been copied, stolen, misused, or even altered. News of data spills, investigations, or lawsuits, widely reported in the press, have caused public relations disasters and disruption of the company's activities. Disputes and civil litigation (mostly in the form of class actions) have ensued.

Government enforcement actions have taken place. In the United States, the Federal Trade Commission (FTC) and state Attorney General offices have conducted investigations of companies' data management practices, which

¹ Copyright 2006 Françoise Gilbert, IT Law Group, Palo Alto, CA. All rights reserved.

Françoise Gilbert is the founder and CEO of IT Law Group, www.itlawgroup.com, a law firm based in Palo Alto, California. A practicing attorney, Ms. Gilbert focuses on the information technology and ecommerce markets. She has assisted global companies and selected start-ups on leading-edge technology legal issues, including data governance-information privacy, information security, and other data management issues.

Ms. Gilbert holds a graduate degree in Mathematics from Paris University (France) and law degrees from Paris University (France) and Loyola University in Chicago (Illinois). She is admitted to practice in California, Illinois, and France.

have resulted in fines and other penalties when deficiencies were identified. Companies that were found to have deficient data protection practices incurred substantial expenses, and were required by court order to implement costly changes. Abroad, foreign data protection agencies have investigated local companies, including subsidiaries of U.S. companies within their jurisdiction, as well.

The increased awareness of the public and the legislators of the problems caused by breach of security, and the necessity to bring company's attention to the need for structured security programs has prompted the enactment of federal and state laws. In the past few years, the legal landscape has dramatically changed. While ten years ago there were almost no laws addressing information privacy or security, today hundreds of state or federal laws attempt to regulate the field and define responsibilities for information holders.

As data privacy and security law and regulations evolve and develop, companies must understand and appreciate the obligations resulting from having the custody of third parties' personally identifiable information, and their compliance obligations. They must also carefully examine the risks and exposure to liability and litigation that might result from failure to comply with the applicable legal requirements, or from failure to provide adequate protection to the personal information in their databases.

This article provides an overview of selected information security issues that affect companies doing business in the United States or globally. Practical suggestions are provided for design and implementation of an Enterprise Security Program and for weaving information security concepts in transactions by performing due diligence and audits, and by incorporating relevant provisions in contracts.

BACKGROUND

Privacy laws regulate the use and disclosure of, and access to, nonpublic personally identifiable information that pertains to an individual – often designated as “data subject.” Among other things, privacy concepts generally require the holder of the protected information to keep it confidential, to use it for specific purposes only, and to share it only with individuals who have the need to know.

To ensure the confidentiality, integrity, and availability of personal or corporate information companies must implement adequate security measures, from fences and locks to passwords, encryption, and firewalls. In

some cases, the requirements are described in laws or regulations. For example, information security concepts have been introduced in regulations drafted by government agencies, such as the Department of Health and Human Services, the Federal Trade Commission, and many others.

States have enacted laws that address information security issues. For example, California requires businesses to use safeguards to ensure the security of the personal information (name plus Social Security Number, driver's license or state ID number, or financial account number) of California residents and to contractually require third parties to do the same.

Criminal laws define penalties for those who gain unauthorized access to protected information or protected computer systems and computer networks. These include, for example, computer crime laws, such as the Computer Fraud and Abuse Act of 1986 (as amended), the Electronic Communications Privacy Act of 1986, or the Computer Security Act of 1987.

In addition, jurisprudence and case law are framing checklists for enterprise security programs. In the meantime, standards setting organizations or government agencies are publishing guidelines to define recommended security measures adapted to the current landscape. The OECD, for example, has established Guidelines for the Security of Information Systems and Networks² and has recommended that these guidelines be used by governments, business, other organizations, and individual users who develop, own, provide, manage, service, and use information systems and networks.

SELECTED INFORMATION SECURITY LAWS AND RULES

INFORMATION SECURITY IN THE HEALTH CARE INDUSTRY

The laws and regulations that govern the protection of health care information are most detailed and comprehensive. Until the mid 1990's, with some exceptions, such as Medicaid or Medicare systems, state laws traditionally governed most matters surrounding health care. However, workforce mobility, the growing inconsistencies amongst state health care laws, the evolution of the insurance industry, the increased use of interstate communications, and other national priorities forced the federal government to increase its involvement in the regulation of health care matters.

² http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html

Passed in 1996, the comprehensive Health Insurance Portability and Accountability Act (HIPAA) attempted, among other things, to respond to the growing public concern over the protection of medical records. HIPAA required the creation of statutes or regulations that would address the privacy and security of patient medical records. To preserve the balance between federal and state laws, HIPAA provided a framework for the concurrent existence of state and federal laws. HIPAA preempts state laws that address the same issues, only to the extent that they provide less protection. If state law would provide more protection, then state law controls.

The HIPAA Privacy Rule³ restricts the use and disclosure of patient health information, outlines patient rights, and defines administrative obligations for covered entities. The Rule applies to specific "covered entities," which are health plans, health care providers, and health care clearinghouses. It imposes restrictions on the use and disclosure of patient individually identifiable information and defines when and whether an authorization is required, whether disclosure to third parties is permitted, or even mandatory.

Any person or company that provides services to the covered entities and that may be handling or getting access to patients' protected information must be aware of the provisions that pertain to the use of "business associates". For example, a company that provides security, legal, or accounting services might be a business associate. A covered entity must enter into a written contract with its business associate. In this agreement, the business associate must give assurances that it will protect the patients' protected health information and assist the covered entity in handling its duties and obligations with respect to such information. If the vendor fails to comply with these requirements, the covered entity must terminate its contract with the vendor.

Published in February 2003, the HIPAA Security Rule⁴ lists the measures that the covered entities must take to protect the confidentiality, integrity, and availability of the protected health information in electronic form in their custody or while transmitting it to third parties. These measures include administrative, physical, and technical safeguards. Security policies and

³ 45 CFR §§ 160.103 et seq. and 45 CFR §§ 164.102 et seq.

⁴ 45 CFR §§ 160.103 et seq. and 45 CFR §§ 164.102 et seq.

procedures, and organizational and documentation requirements are mandated.

CATEGORY	STANDARDS
Administrative Safeguards	Security management process
	Assigned security management responsibility
	Workforce security
	Information access management
	Security awareness and training
	Security incident procedures
	Contingency plan
	Evaluation
	Business associates contracts
Physical Safeguards	Facility access controls
	Workstation use
	Workstation security
	Device and media controls
Technical Safeguards	Access control
	Audit controls
	Integrity
	Person or entity authentication
	Transmission security

The Administrative Safeguards include requirements for the implementation of security management process, assigning security management responsibility, and establishing workforce security. Covered entities must implement information access management, as well as security awareness and training. Security incident procedures with documented report and response procedures must be in place to ensure that security violations are reported and handled promptly. A contingency plan must be in effect for responding to system emergencies, with a data backup plan, disaster

recovery plan, and emergency mode operation plan. In addition, the covered entity must obtain satisfactory assurances from its business associates that they will appropriately safeguard the information in their custody in accordance with these standards.

The Physical Safeguards include facility access controls, and control of workstation use, workstation security, and other device and media. For example, a covered entity must implement policies and procedures to document modifications to the physical components of a facility that are related to security, such as hardware, walls, doors, and locks. Each organization must also put in place physical safeguards to secure workstations and control the use of other equipment. This would involve, for example, policies and procedures that govern the receipt and removal of hardware and/or software (e.g., diskettes and tapes) into and out of a facility.

The Technical Safeguards require policies and procedures for access control, which would involve, among other requirements, the use of unique user authentication and emergency access procedures. Audit controls and mechanisms to authenticate the persons or entities sending the data are also required. Mechanisms to authenticate electronic data and ensure data integrity must be implemented, as well as methods for ensuring transmission security.

The final responsibility for a covered entity's security must be assigned to one official, who will manage and supervise the personnel and the use of security measures to protect data. The covered entities must implement written policies and procedures, review these policies and procedures periodically, and update them as needed. They must also document in writing their actions, activities, or assessments taken or conducted. All documentation must be retained for six years from date of creation or from the date when last in effect.

Finally, HIPAA's provisions with respect to business associates requires service providers that satisfy the definition of a "business associate" to agree to comply with specific confidentiality or security requirements.

INFORMATION SECURITY IN THE FINANCIAL INDUSTRY

Numerous federal and state laws regulate the handling of financial information. These include, for example, the Right to Financial Privacy Act,⁵

⁵ 29 U.S.C. 3401 et seq.

the Financial Modernization Act⁶ (Gramm-Leach-Bliley), the Fair Credit Reporting Act,⁷ and the recent Fair and Accurate Credit Transactions Act of 2003 (FACTA).⁸ These laws limit the ability of businesses to collect and disseminate financial information such as credit information and credit worthiness information. There are also many state laws and regulations.

The Gramm-Leach-Bliley Act (GLBA) contains several privacy-related provisions that apply to all "financial institutions". The Security Safeguards enacted under GLBA define security obligations.

The GLBA reaches a broad range of entities offering financial advice, credit counseling, credit cards, data processing, investments, lending, check cashing, wire transfers, tax preparation, debt collection, or providing credit, insurance, lay-a-way, financing, brokerage, financial aid, lease, or account services. Many companies, such as equipment manufacturers, value-added resellers, and hosted exchanges may be subject to GLBA's privacy and security requirements, as well. In addition, the provisions also affect third parties that do not meet the definition of a financial institution, but that provide services to, and receive nonpublic personal data from financial institutions with which they are not affiliated.

GLBA requires the entities subject to the Act to implement substantial security measures. The agencies that implement GLBA have published separate sets of security regulations implementing GLBA's requirements: the Securities and Exchange Commission (SEC)⁹, Treasury¹⁰, Treasury Office of Thrift Supervision¹¹, Federal Deposit Insurance Corporation (FDIC)¹², Federal Trade Commission (FTC)¹³, Federal Reserve Board¹⁴, Office of the

⁶ 15 U.S.C. §§ 6801-6827.

⁷ 15 U.S.C. § 1681 et seq.

⁸ Pub. L. No. 108-159 (2003).

⁹ 17 CFR Ch. II, Part 248, et seq.

¹⁰ 12 CFR Ch. III, Part 40, et seq.

¹¹ 12 CFR Ch. V, Part 573, et seq.

¹² 12 CFR Ch. III, Part 332, et seq.

¹³ 16 CFR § 313, et seq.

¹⁴ 12 CFR § 216, et seq.

Comptroller of the Currency (OCC)¹⁵, National Credit Union Administration (NCUA)¹⁶, and Commodity Futures Trading Commission (CFTC)¹⁷.

The GLBA Security Safeguards outline the requirements for a company's information security plan. For example, Section 314.4 of the GLBA Security Rule published by the FTC requires that the entity¹⁸:

- **Designate an employee to coordinate the information security program;**
- **Identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, distribution or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks;**
- **Design and implement information safeguards to control the risks identified through the risk assessment phase, and regularly test or monitor the effectiveness of the safeguards' key control, systems and procedures; and**
- **Evaluate and adjust the information security program in light of the results of the testing and monitoring.**

In addition, entities subject to GLBA must require their service providers, by contract, to implement and maintain similar safeguards. For example, Section 314.4(d) of the FTC Security Rule states that in order to develop, implement, and maintain an information security program under GLBA, an entity must:

- (d) Oversee service providers, by:**
- (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and**

¹⁵ 12 CFR Part. 40.

¹⁶ 12 CFR Part. 716.

¹⁷ 17 CFR Part. 160.

¹⁸ GLBA Security rule issued by the Federal Trade Commission. www.ftc.gov/os/2002/05/67fr36585.pdf.

(2) Requiring [its] service providers by contract to implement and maintain the specific security safeguards listed in the FTC rule.

As a result, contracts with third parties must contain clear, specific guidelines, which provide a floor and define a standard for security measures to be taken when processing the data entrusted to these third parties.

SECURITY OF THE PERSONAL INFORMATION OF CHILDREN UNDER 13

The Children's Online Privacy Protection Act¹⁹ (COPPA) governs what information online businesses may collect about children younger than age 13, and the extent to which they can use that information. COPPA imposes certain requirements on website operators and online service providers that collect "personal information" (such as name, address, e-mail address, or other identifying information).

COPPA applies to the collection of children's information online and the subsequent uses of that information. Its primary goal is to give parents control over what information is collected online from their children and how such information may be used.

COPPA also applies to websites with a general audience where the website operator has actual knowledge that the site collects information from individuals younger than 13 and operators of general audience sites that have a separate children's area and that collect personal information from children younger than 13. Among other things, COPPA requires operators to maintain the confidentiality, security, and integrity of personal information collected from children²⁰. Section 312.8 of the COPPA Regulation requires companies subject to COPPA to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

A website operator subject to COPPA must have adequate policies and procedures for protecting children's personal information from loss, misuse, unauthorized access or disclosure.

The Rule does not suggest any specific measure, such as the use of secure web servers or firewalls. Instead, it allows operators to choose from a number of appropriate methods of implementing this provision.

¹⁹ 15 U.S.C. §§ 6501, et seq.

²⁰ 16 CFR Part 312, §312.3(e) and §312.8

The FTC and state Attorney General offices have actively monitored compliance with COPPA. Several companies were prosecuted for improperly gathering and using children's information. For example, in February 2003, Mrs. Fields Cookies and Hershey Foods Corporation each settled FTC charges that they violated COPPA by collecting personal information from children without first obtaining the proper parental consent. Mrs. Fields agreed to pay civil penalties of \$100,000 and Hershey \$85,000. The settlements bar future COPPA violations and require that the companies delete any information collected in violation of COPPA. In addition, the companies must implement record-keeping requirements to allow the FTC to monitor compliance.

THE EFFECT OF THE SARBANES-OXLEY ACT

Although it is not an information security law per se, the Sarbanes-Oxley Act has had a substantial influence in bringing companies' attention to the need for information security measures. In effect, Sections 302, 404, and 409 of the Sarbanes-Oxley Act require public companies to ensure that they have implemented appropriate information security control for their financial information.²¹ By providing that CEOs and CFOs must attest to the quality of the financial data provided to the SEC and shareholders, the Sarbanes-Oxley Act has caused company management to focus on data collection, reporting, monitoring, and supervision, provoking in turn a massive revamping and updating of many public companies' information security procedures.

Section 302 requires that company management certifies the financial information provided in the company's quarterly and annual reports; section 404 requires that companies establish and maintain an internal control structure and procedures for financial reporting, and provide an assessment of the effectiveness of these controls. Section 409, in addition, provides for real-time disclosures of material changes in the financial condition and operations of the issuers.

STATE INFORMATION SECURITY LAWS

In addition to the information security requirements imposed by federal laws, state laws are also beginning to require the implementation of security measures. For example, since January 1, 2005, California requires, with a few exceptions, all entities that own or license contain personal information about a California resident to implement and maintain reasonable security procedures and practices to protect the personal information from

²¹ *Sarbanes-Oxley Act, Pub. Law. 107-204 (2002).*

unauthorized access, destruction, use, modification, or disclosure²². The law also requires companies to ensure through written agreements, that their service providers will also have in place and maintain similar "reasonable" security measures.

The scope of this law is narrow. The protected information includes an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (a) Social Security number; (b) driver's license number or California identification card number; (c) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (d) individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional. Information that is lawfully made available to the public from federal, state, or local government records is not protected by this law.

The California law specifically addresses the retention of third-party service providers²³. If an entity discloses personal information about a California resident to a nonaffiliated third party, it must contractually require the third party to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Consequently, companies that hold California resident's data that is protected under this law must ensure that, when they use service providers, their services agreement contain the necessary provisions to impose on the provider the adequate security measures. Concurrently, organizations that are contemplating transactions with companies subject to this law should be aware of this requirement and plan adequately to ensure that they will be able to satisfy the need of their clients or prospects.

THE NEW REGIME UNDER STATE SECURITY BREACH DISCLOSURE LAWS

Since the enactment of the California's Identity Theft Act (also known as SB 1386)²⁴ in 2003, more than 34 other states have enacted laws that require entities that hold personal data pertaining to residents of their states to notify these individuals of computer security breaches that expose their

²² *California Civil Code Section 1798.81.5*

²³ *California Civil Code Section 1798.81.5(c)*

²⁴ *California Civil Code Sections 1798.29, 1798.82 and 1798.84.*

personal data²⁵. Typically²⁶, these laws require a business that maintains computerized data that includes specified personal information of residents of that state to disclose any breach of the security of that data to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

By requiring that consumers receive such notice, the law intends to give them the opportunity to take proactive steps to ensure that they limit the consequence of the loss of their financial information and do not become victims of identity theft. Several similar bills have been introduced in the US Congress, but none has yet become final. It is likely, however, that there will be soon a federal law that covers this topic and that supersedes the provisions of the related state laws.

The California data breach disclosure law affects any person, business, or organization that conducts business in California and owns or licenses computerized data that includes California residents' personal information. It also affects entities that maintain computerized personal information of California resident. The California law requires the affected entities to notify their California customers if a breach of security occurred (or is suspected to have occurred) that resulted in the unauthorized access to the customers' data.

The law defines a "breach of security of the system" as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. The affected entity must disclose any breach of security following discovery or notification of the breach to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosures to the affected customers must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measure necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

²⁵ For a current list of the states that have enacted these laws, visit the website of the IT Law Group at www.itlawgroup.com.

²⁶ While there are substantial similarities between these laws, there are slight differences worth noting. It is impossible to analyze each of them for the purpose of this article. The remainder of this section is based on the requirements of the California law.

In the case of an entity that maintains information on behalf of another, this entity must notify the owner or licensee of the information of any breach of security immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Under California law, two requirements must be satisfied for a notice to be given to an individual. First, the security breach must expose an individual's first name or first initial and last name in combination with any one or more of the following data elements: Social Security number; driver's license number or California identification card number; or account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Publicly available information that is lawfully made available to the public from federal, state, or local government records is not protected by the law.

The second requirement for triggering a notice is that either the name data or the other data elements must not be encrypted at the time of the security incident. The law, however, does not provide guidance as to the nature of the encryption (i.e., where or how encryption is to be applied).

The California law requires notice to be provided in writing. Electronic notices are appropriate only to the extent that the notice provided is consistent with the provisions regarding electronic records and electronic signature. The law also provides for substitute notice, if the affected entity can demonstrate that the cost of providing notice would be too onerous (more than \$250,000 expense or affecting more than 500,000 persons). In this case, substitute notice is acceptable. The substitute notice may be given by e-mail, conspicuously posted on the website, or made through major statewide media. The California law creates a safe harbor for companies that have their own notification procedures in place as part of their information security policy. However, the notice must be given within the time frames required by the law.

Companies face some challenging questions in determining what types of security incidents may trigger the notice requirements and what kinds of security control they must implement to provide appropriate protection to the relevant personal information.

With more than 34 states having enacted similar – but slightly different – laws, it is clear that should a vendor be the victim of a breach of security, prompt disclosure to the customer would be necessary. The difficulty in compliance for the vendor – and customers as well – is to understand the

requirements of all 34 + state laws, and be able to find a common threshold for what triggers the notice requirements. In addition, each state law may have different reporting requirements. The formalities of making the appropriate disclosure in compliance with the applicable state law, depending on the residence of the customer or the business is definitely a substantial and material challenge.

THE CRUCIAL ROLE OF THE FEDERAL TRADE COMMISSION AND THE STATE ATTORNEY GENERAL OFFICES IN DEFINING INFORMATION SECURITY REQUIREMENTS

The FTC and State Attorney General offices have taken an active role in addressing online security as a consumer issue. Although companies expect that failure to comply with data protection law would expose them to liability, they may be surprised by an FTC or Attorney General's investigation of their information management practices, when no specific law applies to them, and in particular, the level of security provided to personal data. Nevertheless, in the past few years, the FTC and State Attorneys General have been very proactive in investigating companies.

Even if a company is not subject to any specific data protection law, it risks prosecution, fines, and other obligations if it fails to provide a reasonable level of protection to this data, as determined by the Federal Trade Commission. These violations come under Section 5 of the FTC Act, which prohibit "unfair or deceptive business practices" (or equivalent provisions in State "mini FTC Acts", which also prohibit unfair and deceptive practices).

In recent years, numerous well-known companies were prosecuted for privacy or security violations by the FTC, such as Guess.com Inc., Microsoft, Eli Lilly and Company, Tower Records, Petco, BJ Wholesale, DSW, and Choice Point. Lesser-known companies were also investigated and fined (e.g., Educational Research Center of America Inc., Student Marketing Group Inc., International Outsourcing Group Inc., Focus Medical Group Inc., Trimline Inc., and Affordable Accents Inc.).

State Attorneys General have also prosecuted companies for privacy or security violations, either in conjunction with similar FTC actions or independently. For example, the New York State Attorney General has prosecuted Ziff Davis Media, the American Civil Liberties Union, and Victoria's Secret for false claims about data security and Datran Media for inappropriate transfer of user information.

Initially, the prosecutions were conducted under the "deceptive practices" prong of Section 5 of the FTC. The FTC ruled that for a company to post

privacy policy that assures the consumers that it is using "the highest security available" (or similar statements) was deceptive if the company's security was not consistent with best practices.

Recently, however, the FTC has increased pressure on organizations by creating a "per se" approach. Failure to provide reasonable security for consumer's information has become a "per se" violation of the Article 5, because the FTC views it as "an unfair practice" to collect individual's information and fail to protect this information with a reasonable level of security.

Thus, even when a company is not directly regulated by specific information privacy or security laws, it is susceptible of prosecution by FTC and State attorney general, for it's handling of personally identifiable information, or inadequate information security protection. Organizations that process personally identifiable information must urgently implement a company wide information security plan to ensure that the personal data are adequately protected. In addition, before entering into a relationship with a service provider that would process these personal data, proposed data collectors should conduct appropriate due diligence to evaluate whether the proposed service provider has in place the policies and procedures needed to protect personal information and will fulfill other obligations related to the handling of individuals personal information.

Current rulings by the Federal Trade Commission after determining that a company had deficient security measures include the following requirements:

- **Identify a responsible party:** *the designation of an employee or employees to coordinate and be accountable for the information security program*
- **An Asset Assessment:** *the identification of the systems and information that need to be protected*
- **A Risk Assessment:**
 - *The identification of material internal and external risks to the security, confidentiality, integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction or other compromise of the information.*
 - *The assessment of the sufficiency of any safeguards in place to control these risks*
- **Development of Security Measures:** *the design and implementation of reasonable safeguards to control the risks identified through the risk assessment phase*

- **Testing and Monitoring:** *the regular testing and monitoring of the effectiveness of the safeguards, key controls, systems, and procedures*
- **Periodic Audits and Adjustments:** *the evaluation and adjustment of the information security program in light of the results of the testing and monitoring, any material changes to the company's operations or business arrangements, or any other circumstances that may have a material impact on the effectiveness of the company's information security program.*

The list above can serve as a checklist of activities when designing a company's security plan, policies and procedures.

DOING BUSINESS ABROAD: INFORMATION SECURITY LAWS OF WORLD – OR ABSENCE THEREOF

If a company contemplates the need to receive or process personal data protected by foreign laws, it should anticipate the need for compliance with those laws. Thirty-five years after the first data protection law was enacted, more than 50 countries now have substantial data protection laws. These laws are relevant to U.S.-based companies with global operations. Foreign subsidiaries, suppliers, agents, or other subcontractors of U.S. corporations are subject to the jurisdiction of the countries in which they are located. Any use of their databases is controlled by the local laws. Attempting to transfer the databases to a third party in a foreign country may be problematic if there are restrictions in the local data protection law.

- **European Union and European Economic Area**

All countries in the European Union (EU) and the European Economic Area (EEA)²⁷ have enacted data protection laws that restrict the collection, use, and dissemination of personal information. Although there are discrepancies, each country's data protection law follows the guidelines set forth in the EU Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data.²⁸ Data protection laws are also being updated

²⁷ *The European Union has 25 members: Austria, Belgium, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, the Netherlands, and the United Kingdom.*

The European Economic Area (EEA) comprises Norway, Iceland, Lichtenstein, and the countries that are members of the European Union.

²⁸ http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.

to implement the EU Directive 2002/58/EC for the Protection of Personal Data and Privacy in the E-communications Sector (which supersedes its prior EU Directive 97/66/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector).²⁹ This 2002 directive mandates restrictions with respect to spam, telemarketing and interception of communications, traffic data, and customers' personal data.

In particular, each EU Member State has implemented into its data protection law Article 17 of the 1995 Data Protection Directive, which addresses the security of personal information and requires companies to implement reasonable security measures to protect the personal data in their custody.

Article 17 provides:

Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

²⁹ http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.

- ***the processor shall act only on instructions from the controller,***
 - ***the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.***
- 4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.***

Article 17 is implemented, for example, in the Data Protection Act of the United Kingdom in the Seventh Principle, which states:

7. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Information security is indeed an integral part of data protection in the EU and EEA. Thus entities doing business in the EU or EEA, or receiving data from the EU or EEA countries must be aware of the need to have adequate information security measures in order to comply with the local laws of the relevant EU or EEA member state.

Using its power, similar to those of the FTC or the State Attorney Generals in the US, Data Protection Authority of a EU or member state can take action against the collector or data processor, including imposing administrative fines or sanctions and prison terms. Data Protection Agencies in EU member states have dragged subsidiaries of U.S. corporations into court over the misuse of data.³⁰

Information Security Requirements when Exporting Personal Data from the European Union

US entities must be especially cognizant of the provisions in the data protection laws of EU member states that prohibit transfers of personal information outside the EEA unless the entity transferring the data has obtained "adequate" assurances from the data recipient that the personal information and the data subjects will receive at least the same level of

³⁰ *The Spanish Data Protection Agency, for example, has found Microsoft liable for violation of the Spanish Data Protection Laws and assessed a \$57,000 fine for unauthorized transfer of personally identifiable information outside of Spain.*

protection in that foreign country as they do in the EU or EEA country where the database was created.³¹

The company may need to obtain specific permission from the data subjects before transferring content in its databases outside of the EU or EEA. The parties exchanging protected data may have to enter into specific contracts for the transfer of personal data. The recipient of the personal data may have to commit to privacy and security procedures that are consistent with the local law. The proposed transaction may face the scrutiny of the local Data Protection Agency.

Data pertaining to EU residents may not be exported to the United States or most countries outside of the EU if there is not a specific commitment from the data recipient that it will provide the data subjects with the rights and protections consistent with those that are offered in the EU. Several methods are available to provide these "adequate assurances": (1) self-certification under the Safe Harbor program; (2) using model contracts that have been approved by the European Commission; or (3) use of a code of conduct.

Each of these methods requires the US company (or other non-EU recipient) to commit provide adequate security to the data it would receive from a company located in the European Union.

Safe Harbor

The Safe Harbor program has been developed after lengthy negotiations between the U.S. Department of Commerce and the European Commission.³² Only entities that are subject to the regulation of the FTC and the Department of Transportation may benefit from the safe harbor program. This restriction excludes banking and credit institutions and others, for example.

In addition, this program only applies to US companies. Thus, if a US company wishes to transfer personal data from the EU to its call center in India or the Philippines, it cannot do so under the Safe Harbor program. Instead, there would need to be a contract between the EU data exporter and the call center.

³¹ *The Data Protection Laws of each of the country members of the EU contain provisions that incorporate the mandate of Article 25 and 26 of the 1995 EU Data Protection Directive.*

³² www.export.gov/safeharbor/index.html.

For a US company, self-certifying under the Safe Harbor system assures the EU data exporter that the U.S. Company provides "adequate" privacy protection, as defined by the Directive. Once the U.S. Company has joined the safe harbor program, it receives a presumption from all EU member states that it offers the required "adequate protection" of personal information in a manner consistent with the protection that is granted in the EU member states.

To qualify for Safe Harbor, a U.S. company must self-certify that it abides by a number of principles. One of them pertains to information security. The US company must represent that it has in place reasonable security to protect the data.

Of course, the U.S. Company must act in accordance with the representations made as part of the certification process, or it risks prosecution under U.S. laws.

In addition, the foreign company that would be transferring information to the U.S. Company still needs to comply with its own data protection law as well, and both EU and U.S. companies must enter into the proper written agreements to define the proper uses of the transferred data.

Model Contracts

An alternative to Safe Harbor self-certification is the use of written agreements between the data importer and the data exporter. The European Commission has published two sets of model contracts that must be used verbatim, without modifications. These contracts are between the data exporter (located in the EU) and the data importer (located in the United States or other non-EU country). Among other things, these contracts define the responsibilities of the parties, make the European individual a third-party beneficiary, and require the data importer to commit to providing the individual data subjects with substantially the same rights and protections as those enjoyed in their country of residence. In addition, the US Company must commit to protect the imported data with adequate security measures.

If a global company elects to use the model contracts in order to export EU data to the United States, it will have to ensure that it has in place sufficient information security measures to satisfy this provision of the Model Contract.

Binding Corporate Rules

The third alternative is the use of binding corporate rules (i.e., the use of codes of conduct instead of model contracts for the transfer of personal data to third countries). This process is not yet widespread because it is cumbersome and requires review and approval by the data protection agencies, which makes it a cumbersome and lengthy process. However, to the extent that BCR are used (after approval by the relevant Data Protection Agency) a security component must also be used to comply with Article 17 and the local EU member laws.

- **Information Security Outside of the EU and EEA**

Outside the EU and EEA, most countries that have enacted data protection laws have followed data protection principles substantially similar to those in the guidelines drafted by the OECD,³³ the United Nations (UN)³⁴ or the EU. As a result, many foreign data protection laws also impose some restrictions on the transfer of data to third parties. For example, the Australian Federal Data Privacy Law restricts the transfer of personally identifiable information to any third party if the data subject has not been informed in advance that such transfer might occur.³⁵

It is not possible to describe in detail here the Data Protection laws in other parts of the world. The tremendous influence of the 1995 EU Directive, however, is clear. Many countries outside of the EU have opted to follow the model created by the European Commission so that their own country's law is consistent with the EU Data Protection Directive, and their constituents do not face substantial hurdles when attempting to exchange personal data with EU companies. As a result, in more than 40 countries, the collection of personally identifiable information from individuals, as well as the manipulation, correlation, disclosure, transmittal, and other data processing, are heavily regulated. Examples include, in addition to the 25 EU members and EEA countries, Argentina, Australia, Brazil, Bulgaria, Canada, Chile, Hong Kong, Israel, Japan, New Zealand, Paraguay, Russia, Switzerland, and Tunisia. Although these countries may not offer data protection and rights as substantial and comprehensive as those defined in the EU Data Protection

³³ www.oecd.org.

³⁴ www.un.org.

³⁵ See, e.g., Australian Federal Data Privacy Law: www.privacy.gov.au/publications/ipps.html

Directive, in most circumstances, their data protection laws includes provisions that require that adequate security be provided to personal data.

About 75 percent of the countries in the world lack privacy protection. In some of these countries, bills might be pending, but it is unclear when or whether a law will be enacted, what it will cover, or how it will be enforced. For example, the Philippines currently has no general data protection law, although a draft has been proposed. According to press reports, the bill would adhere to the EU data protection standards. India, which is a substantial service provider to companies in the US and elsewhere, does not yet have a data protection law, despite several announcements that it was considering a new Data Privacy Act. India's Ministry of Information Technology is said to be preparing a draft in cooperation with the National Association of Software and Services Company. According to press reports, India's proposed law would take into account the floor set by the EU Directive, so that the Indian data protection law satisfies the concern of the EU Commission and ensures that EU companies can outsource services and operations to India.

Elsewhere, despite the general interest for information privacy and security, there is no protection of personal data. This is the case, for example, in Mexico³⁶ and Central America, most of the Middle East (except Israel), Africa, China, Malaysia, Singapore, and most of Asia (except Russia).

The Republic of Korea (South Korea) has adopted the OECD Guidelines, and its constitution provides explicit protection of privacy and freedom from intrusion into correspondence and place of residence. In practice, however, government agencies and private-sector entities are said to pay little respect to privacy rights.

There is no data protection law in Singapore. The government is frequently criticized for surveillance of political opposition groups and ordinary citizens. Singapore has no governmental authority affiliated with privacy or data protection.

Similarly, Malaysia does not specifically recognize a right to privacy, and there has been little progress in the development of a regime for the protection of personal data. The constitution of Malaysia does not recognize the right to privacy. A controversial law, the Internal Security Act, allows police to search without a warrant the homes of persons suspected of threatening national security. They may also seize evidence.

³⁶ *Bills are pending in Mexico, but no law has yet been enacted.*

Even though Hong Kong and Taiwan have data protection laws, the People's Republic of China does not have protection legislation. The Chinese constitution provides for limited rights to privacy. Freedom and privacy of correspondence are protected by law. No organization or individual may infringe on citizens' freedom or privacy of correspondence, except for state security or criminal investigations. Hong Kong, however, has legislation based on the EU Directive, with a personal data ordinance, covering public and private data users. Similarly, the Taiwanese constitution articulates a restricted right of privacy, and the 1995 law on Computer Processed Personal Data Protection governs the collection and use of personal information by government agencies and many areas of the private sector.

A company contemplating the use of personal data when doing business abroad or contemplating the use of outsourcers located off-shores should understand the scope of protection -or lack thereof- in the country where the services would be performed. Obligations to provide security to personal information may stem for a variety of laws. In general, sticking one's head in the sand will cause a viable alternative. Addressing information security obligations will be necessary and required. In countries with complacent law enforcement or a corrupt legal system, other tools may be necessary to prevent the theft or misuse of data entrusted to a service provider.

IMPLEMENTING INFORMATION SECURITY WITHIN THE ENTERPRISE

The global security in the first part of this article shows that companies that collect, process or use personal data should be very attentive to privacy and information security issues. These issues are complex. They require specific detailed knowledge and understanding of the applicable laws, regulations, and other constraints. A cookie-cutter approach can only lead to a disaster. Failure to fully understand the information security constraints and compliance requirements may lead to disruptive litigation and/or unanticipated cost and expenses.

THE INFORMATION SECURITY PLAN

While it is clear that companies are getting a legal obligation to provide adequate security to most personal information they collect, the laws, regulations, and court rulings described above do not specify what specific security measures should be implemented. They merely require that the security be "reasonable," "appropriate," or "adequate." Nevertheless, these laws and the enforcement action initiated by the Federal Trade Commission

and State Attorneys General take a consistent approach to information security. They outline a process leading to the development of a comprehensive security program.

The Consent Decrees issued by the FTC and state agencies after the investigation of a company's security practices have a common theme when addressing information security requirements. This theme is also similar to the provisions of the information security laws that are currently in effect in the United States as well as the guidelines issued by standard setting or professional organizations.

In summary, when planning to design and establish an enterprise security program, a company should consider following the roadmap below:

- **Identify a responsible party**

The company should designate an employee or employees to coordinate and be accountable for the information security program. The Sarbanes Oxley Act, for example, makes the CEO and CFO of a company accountable for the quality of the company data filed with the SEC, and consequently makes them responsible for ensuring the security of these data. The Gramm-Leach-Bliley Act makes the company's Board of Directors responsible for ensuring the implementation of adequate security, while the HIPAA Security Safeguards give this same responsibility to a Security official to be appointed by the company. FTC Consent decrees also require companies to designate an individual to coordinate and be accountable for the company's information security program.

- **Assess the assets to be protected**

The first step is to conduct an assessment of the assets to be protected. This would include, for example, the identification of the systems and information that need to be protected: what data, applications; what information systems, networks. Where are they located? What are the processes used by the company.

It is also crucial at this stage to understand which laws apply to these assets: US federal, state or local Laws, security breach disclosure laws. Other related laws might be relevant as well: search and seizures of evidence, E-discovery laws and document retention and destruction laws

- **Assess the Risk to these Assets**

Once the sensitive assets are identified, the company should identify the material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction or other compromise of the information. The company should identify all reasonably foreseeable internal and external threats to the information assets to be protected. For each identified threat, there should be an evaluation of the risk posed by the threat. For example: the likelihood that the threat will materialize. What potential damage might result from the threat? In addition, there should be an evaluation of the sufficiency of the policies, procedures and safeguards already in place to guard against the threat.

- **Develop Security Measures**

Once the assets and risks to these assets are identified, the company should design and implement reasonable safeguards to manage and control the risks identified through risk assessment.

The Information Security Plan should be in writing, coordinated between the different parts of the company and appropriate for the particular organization. The measures, policies and procedures to be used should be adapted to the probability of potential risk, the company's size, capabilities, the nature and scope of activity, and the sensitivity of information to be protected.

The laws, regulations, and consent decrees do not identify specific measures. The company should identify applicable standards and best practices, and choose what is appropriate of its business. There are numerous sources available, such as: the PCI (payment card industry) Standards; The GASSP (Generally Accepted Systems Security Principles); ISO 17799 (International Standards Organization); NIST 800 series; or the HIPPA Security Safeguards.

Typically, these standards require the establishment of physical, technical, and administrative security measures. Physical Security Measures would include, for example, physical facilities and device access control. Technical Security Measures would include, for example, procedures for granting and controlling access, or terminating access to computers, networks or databases; intrusion detection procedures; system modification procedures; or measures to ensure data integrity and confidentiality, or precautions to be taken when storing or destroying data. Administrative Security Measures would focus on items such as the retention, storage, and destruction of

documents; the use of audit controls, such as to record modifications to documents.

The plan should also include a code of conduct for the personnel in order to create rules for discipline and sanctions against the employees who fail to comply with the security policy.

There should be procedures designed to ensure the ability to continue operations in the event of an emergency. To ensure compliance with the data breach disclosure laws, the company should also draft an Incident Response Plan. This plan would outline an organization for taking responsible action if the company suspects a security breach, or detects that a security breach has occurred.

In addition to its own information security, a company should ensure that similar measures are taken by the third party to whom it provides its sensitive data, such as service providers, outsourcers and the like. Indeed, regardless of who performs the work, the legal obligation to ensure security of information remains with the company. The company should exercise due diligence in the selection of service providers. It should also contractually require the service providers to implement appropriate security, monitor the performance of the service provider; and if needed, terminate the relationship.

- **Implementation and Training**

No plan will be effective unless it is correctly implemented, and understood by the company personnel. Upon completion of the Information Security Plan, the company should communicate to its employees the applicable security policies, procedures, and guidelines. Adequate training should be organized throughout the company. The company should also implement security awareness program, which should include the distribution of periodic reminders and the provision of refresher training courses to ensure continued compliance.

- **Audit, Test and Monitor**

To ensure compliance with its Information Security Plan, the company should also regularly test and monitor the effectiveness of the safeguards, key controls, systems, and procedures. These periodic tests are intended to ensure that the security measures are properly in place, and are effective. Audit logs, access reports, incidents tracking reports should be reviewed.

The tests should also include an evaluation of personnel compliance with the program.

- **Conduct Periodic Revisions and Adjustments**

The company's information security program should be periodically adjusted and modified to take into account the results of the testing and monitoring, any material changes to the company's operations or business arrangements, or any other circumstances that may have a material impact on the effectiveness of the company's information security program.

Changes to the current information security plan should also take into account any changes in technology, and in internal and external threats (e.g. new forms of cyber crime).

RELATIONSHIP WITH SERVICES PROVIDERS

An information security plan is not complete if a company does not also address security in its relationship with its service providers. The potential information security issues should be addressed before entering into or negotiating an agreement with any entity to which the company provides personal data for processing or other uses, as well as any company from which the company receives personal data. As part of its due diligence, the company should identify and understand the privacy and information security issues involved. Addressing these issues early on may prevent unnecessary disruption and waste of time and resources. The proposed arrangement should be evaluated in light of the respective players' privacy and security policies and other restrictions or commitments before signing the contract.

Essential to a successful transaction is the company's understanding of its data collection and data protection practices, how its databases are created and used, and the policies, contracts, and laws that apply to the use or disclosure of data necessary for its business. If it is contemplated that subsidiaries, affiliates, distributors, or other third parties will use the service provider, the inquiry should include these companies as well. The vendor should conduct a similar evaluation of the proposed customer's practices.

In preparation for a transaction, the parties should analyze whether and how the proposed arrangement may lead to, or require the collection, use, maintenance, or access to private data. If due diligence has identified databases of private information, the parties should determine whether the

entity that will have access to these data has in place the sufficient privacy and security measures that are required by law.

The parties must also evaluate the security needs associated with the specific transaction and whether the service provider has the economic, technical, and human resources necessary to handle the security or other obligations. In addition, the company may want to know whether the laws, judicial systems, and the political climate in the vendor's country will provide sufficient protection consistent with its needs to protect the security of the data it entrusts to the service provider. The company must be assured that the required information security protections and procedures will be in place and respected, consistent with the subject matter of the contract.

The written agreement should define, as appropriate, how data security issues will be addressed during the term of the contract and upon termination. Appropriate clauses might specify the limits to the use or handling of the data, or implementing specific security measures. Allocation of responsibilities, liability obligations, and risk management provisions should be incorporated into the definitive agreement as well. The parties may wish to negotiate covenants or representations and warranties with respect to the data and the scope of use of the data. Indemnification provisions and limitation of liability provisions might be appropriate, to address liability that may result from loss or misuse of data or breach of contract. The customer should plan to conduct periodic audits of data protection practices, to ensure that the service provider complies with the contract.

The contract should also anticipate that new laws will be enacted. Both companies should be concerned about the many restrictions and the need to be informed of the new developments, to ensure that the services agreement is updated as needed.

MONITOR LEGAL DEVELOPMENTS

Information security is in constant evolution. It is a fertile field for new federal and laws and regulations. In addition, the FTC and State Attorneys General remain active watchdogs, and try to ensure that personal data receive adequate protection. As a result, this area is evolving drastically. Consequently, companies should constantly monitor legal and legislative developments.

CONCLUSION

Companies must pay attention to information security. Numerous laws and regulations require companies to have in place adequate security measures. Gramm Leach Bliley Act, HIPAA, COPPA, Sarbanes Oxley Act, and other federal laws are shaping the federal legal landscape. Several state laws, such as California's Civ. Code Sec. 1798.81.5 also require companies to address information security issues. FTC and State AG Orders issued after investigations of companies' security practices are requiring the implementation of a comprehensive information security program. Abroad, the Data Protection Laws of EU Member States also contain an information security requirement. Countries that have followed the EU model, such as Australia or Canada, also impose on data processors the use of appropriate measures to protect the data in their custody.

The information security landscape is constantly evolving, and legal requirements are becoming increasingly stringent. It is clear that the existing laws and the Federal Trade Commission rulings are making **all** companies responsible for the protection of the personal data they collect, store, use, or transfer.

A company's most important assets are its personnel and its customers. It must ensure the safekeeping of these critical assets. To survive and be competitive, the organization must invest the resources necessary to indicate its respect for the information security of personal information pertaining to them. Failure to do so could cause great harm. It is irrelevant if a company's products or services may be the most inventive, creative, or useful, a "little glitch" that results in the loss or exposure of personal information could cause public relations disaster. If there is a security breach, and personal data is disclosed or lost, the existence of this loss will quickly reach the first page of the newspaper. From there, the news will spread to cause great harm to the company's reputation. Class action suits, and/or government agency investigations will follow.

To properly address the complex issues that surround the collection and use of personal information, it is essential to have a thorough understanding of information security laws. Then, it is critical to draft, implement and comply with a well thought out, comprehensive, Enterprise Security Program. The creation of an enterprise security program is a complex process in which legal counsel plays a critical role. The company must assess existing data flows; evaluate risks, and understand its compliance requirements. The next phase is to develop policies (high level) and procedures (for daily use) that take into account the knowledge of which information must be protected, and from which risk it should be protected. When the Plan, Policies and

Procedures are complete, they must be implemented throughout the company. The training of the company's personnel is a crucial step in the success of the implementation. Once all the components are in place, the company must start monitoring the application, and discipline the infringers as they are identified. As time goes by there is a better understanding of the company's needs and obligations, the policies and procedures should be reviewed as necessary, and personnel should be trained periodically, either on existing procedures or on new requirements.

/ Palo Alto – October 22, 2006