Protecting Personal Information in Third Party Hands

An Overview of Legal Requirements

Margaret P. Eisenhauer[1]
6 January 2006

U.S. companies are increasingly subject to fiduciary-like duties with regard to the personal information they collect and maintain from customers and employees. These duties include obligations to protect the personal information with "reasonable security" measures as well as to reasonably prevent any misuse of the information, such as uses outside of a posted privacy notice. The requirements for reasonable security mandate internal security processes along with oversight and control of third party data processors.

This paper explores some of the regulations and regulatory actions that have created security obligations. It does not attempt to provide a comprehensive statement of any set of security requirements. It is merely designed to provide some basic information on the ways that security laws and regulatory actions shape company relationships with third party data processors.[2]

Specific Laws and Regulations

Federal Regulations

We have seen an array of Federal and state laws that impose requirements on companies to protect personal information. At the Federal level, privacy and security regulations historically tied to uses of personal information (such as credit reporting). More recently, laws have been passed to regulate the information handling practices of all companies within certain industries. For example, companies in the following industries are subject to broad and deep requirements regarding their handling of personal information:

---

[1] **Peggy Eisenhauer** is founder of Privacy & Information Management Services – Margaret P. Eisenhauer, P.C., a full-service privacy, security and information management law firm. She helps companies develop, implement, and assess privacy and fair information practices, including policies governing the collection, use and disclosure of customer and employee information. She has extensive experience with U.S. and international privacy and security laws. In addition to a J.D. degree with honors from the University of Georgia School of law, Ms. Eisenhauer has a Masters of Science in Information and Computer Science from the Georgia Institute of Technology. She is a Fellow of the Ponemon Institute, a Certified Information Privacy Professional (CIPP) and a member of the International Association of Privacy Professionals CIPP Advisory Board. *Ms. Eisenhauer is admitted to practice law in Georgia and Florida, U.S.A.* She can be reached via email to peggy@privacystudio.com or via telephone at 404-914-1163.

[2] This article and its attachments have been prepared for informational purposes only and are not legal advice. If you have any questions about any particular legal requirement or your specific processor relationships, please contact your own attorneys or the author for legal advice.

- All companies "significantly engaged in activities that are financial in nature" are subject to the Gramm-Leach-Bliley Act (GLBA) and the attendant Privacy and Safeguards Rules.

- All healthcare providers, health insurance companies and healthcare information clearinghouses are subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, and

- All schools and institutions that receive funds from the Department of Education are subject to the Family Educational Rights and Privacy Act (FERPA).

In each case, the laws require that the subject entity pass the legal obligations on to any entity that accesses or receives regulated personal information from it.

For example, the GLBA Safeguards Rule requires financial institutions to develop and implement a comprehensive information security program that is appropriate to the size, complexity, nature and scope of the activities of the institution and that contains "administrative, technical and physical safeguards" to protect the security, confidentiality and integrity of customer information.[3] The safeguards must be reasonably designed to (i) insure the security and confidentiality of customer information, (ii) protect against any anticipated threats or hazards to the security or integrity of the information, and (iii) protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.[4]

A GLBA-compliant information security program is required to have certain elements, including a designated employee to coordinate it, audit systems to determine risks, and certain procedures to take with service providers to assure the security of the information is maintained. With regard to service providers, the Safeguards Rule specifically requires financial institutions to "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 (2) requiring your service providers by contract to implement and maintain such safeguards."[5]

Similarly, the HIPAA Security Rule set forth strict requirements for all data processors, which are classified under HIPAA as "business associates." The Security Rule states that: "a covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information."[6] The Security Rule then establishes the minimum requirements for all business associate contracts:[7]

---

[3] 16 C.F.R. § 314.1(a)

[4] 16 C.F.R. § 314.3

[5] 16 C.F.R. § 314.4(d)

[6] 45 C.F.R. 164.308(b)(1)

[7] 45 C.F.R. 164.314(a)

> The contract between a covered entity and a business associate must provide that the business associate will—
>
> (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;
>
> (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;
>
> (C) Report to the covered entity any security incident of which it becomes aware;
>
> (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

But even companies that are not subject to a Federal privacy law may well be subject to state privacy or security laws that require it to manage its data processors. State legislators have been passing privacy and security laws to "fill the gap" by imposing regulations on entities not covered by the Federal laws listed above. Federal and state regulators have also developed general theories of liability for failure to have reasonable security as well.

California AB 1950

In 2004, California became the first state to impose a general security standard on businesses that maintain personal information. This law, commonly known as AB 1950, became effective on January 1, 2005. It targets entities that are <u>not</u> covered by GLBA, HIPAA or other similar Federal privacy laws, and it imposes stringent information security requirements on these entities.

A.B. 1950 requires businesses that own or license personal information about California residents to implement and maintain reasonable security procedures and practices to protect the information from unauthorized access, destruction, use, modification or disclosure.

The new law applies to all otherwise unregulated businesses that own or license personal information about California residents, whether customers or employees. "Personal information" means unencrypted data consisting of a person's name, *in combination with*:

- A Social Security number,
- A driver's license or California ID card number,
- An account, credit card or debit card number (with a password or access code if needed), or
- Medical information.

A.B. 1950 requires companies to implement and maintain reasonable security procedures and practices, appropriate to the nature of the personal information, to protect the information from unauthorized access,

destruction, use, modification or disclosure.[8] Additionally, AB 1950 compels businesses to contractually impose security requirements on entities that process data for them.

AB 1950 was enacted to complement California's security breach notification law, SB 1386. SB 1386 took effect in July 2003 and requires companies to notify California residents of any unauthorized acquisition of computerized personal information. SB 1386 defined "personal information" as unencrypted data consisting of a person's name, in combination with:

- A social security number,
- A driver's license or California ID card number, or
- An account, credit card or debit card number (with a password or access code, if needed).[9]

SB 1386 did not itself require companies to protect the personal information, however. It merely required them to notify individuals if the information had been inappropriately acquired. AB 1950 was enacted to impose basic security requirements on companies, so they would have liability if the information lost was not being reasonably protected.

Other State Security Laws

During the past year, 22 states have enacted their own privacy and security breach notification laws. (A list of the states is provided below.) Many of these laws copy SB 1386, although several have additional provisions (such as notification of consumer reporting agencies) and several also require companies to have reasonable security to protect sensitive personal information.

Under these new laws, "personal information" is generally defined as name plus a Social Security number, driver's license number, or financial account information. A few states have expanded the definition of personal information as well. For example:

- Arkansas's law includes medical information,
- Georgia's law[10] does not require name to be connected with the data elements,
- Maine includes other account passwords or identification numbers, it also does not require name to be connected with the data elements,
- North Carolina includes any other personal information, including biometric data and other identifiers, and (most notably)
- North Dakota includes employer identification numbers, mothers' maiden names, and electronic signatures.

---

[8] "Reasonable security procedures" is not defined, but it is generally understood to encompass the types of administrative, physical and technical measures that are described in the GLBA Safeguards Rule.

[9] SB 1386 does not mention medical information. AB 1950 goes farther than SB 1386, by requiring companies to protect medical information as well as the other listed data elements.

[10] Georgia's law only applies to "information brokers" but this term is defined very broadly to encompass any entity whose business includes the collection or compilation of personal information to be furnished to third parties.

Many of these new laws have explicit requirements that companies provide reasonable security for the personal data they possess and share with affiliates and other third parties. Others rely on developing theories of liability for failure to have reasonable security even in the absence of an explicit law. As discussed below, the Federal Trade Commission (FTC) and state attorneys general have developed strong positions that failure to protect personal information (with appropriate security) and respect privacy promises are unfair and deceptive trade practices. With regard to security, even in the absence of explicit requirements, the FTC uses the stringent regulatory approach that it developed for the financial services industry under GLBA.[11]

State security breach notification laws have been enacted in:

Arkansas	Maine	North Dakota
California	Minnesota	Ohio
Connecticut	Montana	Pennsylvania
Delaware	Nevada	Rhode Island
Florida	New Jersey	Tennessee
Georgia	New York	Texas
Illinois	North Carolina	Washington
Louisiana		

While all companies should take steps to ensure that third party data processors appropriately safeguard personal information, companies with information on residents of these should take extra care when passing information to data processors. In particular, companies should examine their data processing contracts to include specific provisions regarding Social Security numbers, employee identification numbers (in North Dakota) or medical/disability information (in Arkansas and California).

Please also note that, in each state listed above, companies (as the data owners) would be required to notify individuals in the event that sensitive personal information was lost, by either the company or a data processor. This notification process is often followed by a regulatory inquiry into the company's security practices (as well as media and client inquiries). If a company is unable to demonstrate that controls are in place around data processors, it could face regulatory action under the applicable state law or other liability theories discussed below.

Specific Restrictions on Social Security numbers

On July 1, 2002, California became the first state to significantly restrict private use of Social Security Numbers (Social Security numbers). California Civil Code 1798.85 prohibits any person or entity from:

(1) Publicly posting or displaying a Social Security number in any manner.

(2) Printing a Social Security number on any card required for the individual to access products or services.

[11] Since GLBA requires "reasonable security," the FTC believes that it is an appropriate general model for all companies.

(3) Requiring an individual to transmit a Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted.

(4) Requiring an individual to use a Social Security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the Web site.

(5) Printing an individual's Social Security number on any materials that are mailed to the individual, unless state or federal law requires the Social Security number to be on the document to be mailed or the mailing consists of a "form or application."

Additionally, entities are generally expected to have reasonable security to protect Social Security numbers because this particular data element is so closely associated with identity theft.

Companies should classify Social Security numbers as a "sensitive data element" so that it receives appropriate protection. The privacy standards are designed to help ensure that Social Security numbers are not intentionally or inadvertently misused by third parties who receive them.

The California Social Security number law has been copied by many states. Other states have added some additional provisions, such as limits on recording Social Security numbers on payment instruments or using Social Security numbers as a general identification number or account number. States that currently restrict private use of Social Security numbers include:[12]

Arizona	Missouri	Utah
Colorado	New Hampshire	Vermont
Georgia	New Jersey	Virginia
Illinois	New Mexico	Washington
Maine	Ohio	West Virginia
Massachusetts	Oklahoma	Wisconsin
Michigan	Rhode Island	

In each of these states, companies should make sure that any entity that receives Social Security numbers agrees to protect those Social Security numbers and comply with the applicable laws. Companies should also ensure that data flows between itself and its processors do not include inappropriate transmissions of Social Security numbers (such as via the mail or transmissions over the Internet in unencrypted formats).

Regulatory Expectations – Unfair Trade Practices Liability

Even absent a specific law, companies are required by the FTC to have reasonable safeguards in place to protect sensitive personal information, including credit card numbers, medical information and Social Security numbers. The FTC is actively bringing enforcement actions against companies that fail to employ reasonable security for personal information. These actions are brought under its general jurisdiction to restrict unfair and deceptive trade practices. State attorneys general are also bringing actions under similar theories. These FTC and state attorney general actions have created a *de facto*

[12] A number of states limit government use of Social Security numbers. These laws do not affect private entities directly.

national requirement that companies implement appropriate privacy and security programs, including vendor and employee oversight.

Historically, FTC actions were styled as deceptive trade practice cases, with the FTC alleging that the company failed to honor promises made to consumers. (For example, the FTC has brought actions against companies for failing to live up to statements made on websites regarding "reasonable security.")

The FTC has now expanded its arsenal, alleging that companies' security breaches are the result of unfair trade practices. In recent complaints against companies that have suffered security breaches, the FTC has filed complaints alleging that the companies' failures to employ reasonable and appropriate security measures is unfair because it could cause substantial injury to the individuals that is not offset by any countervailing benefits to the individuals and that cannot reasonably be avoided by the individual.[13]

To avoid FTC action, companies must also prohibit data processors from using personal information in any manner that is inconsistent with the companies' published privacy notices. In other words, when a company collects personal information subject to a published privacy notice, it cannot permit any third parties to use the personal information for any purpose that contravenes the notice.[14] As the FTC has opined, companies and data recipients must be "in sync" – data recipients cannot do things that exceed the scope of the companies' privacy notices, and companies must know and manage the actions of their data recipients.

Any failure to protect data from loss or misuse is potentially an unfair and deceptive trade practice. Companies should therefore use their data processing contracts or service agreements to inform their data processors of the appropriate scope of their use of the company's personal information as well as their obligation to reasonable safeguard the data from loss or unauthorized access.

Attachment 1 to this paper contains a summary of the provisions that the FTC has included in several recent consent decrees associated with privacy and security breaches. These consent decree terms illustrate the types of provisions that the FTC imposes on companies that have had issues resulting in FTC attention. The onerous nature of these provisions has helped many companies understand that an upfront investment in privacy and security – including employee and vendor oversight – is essential to avoid the risks of a consent decree.

Conclusion

Companies today have fiduciary-like duties towards the individuals who entrust their information to them. Companies must, as a matter of law, provide reasonable security for the information and ensure that the information is used appropriately, in accordance with its privacy notices. This means that they must develop and implement robust information security programs that include management of third party processors.

---

[13] See, *e.g.*, FTC actions against DSW Shoe Warehouse, BJ's Wholesale Club, linked from http://www.ftc.gov/privacy/index.html

[14] See, *e.g.*, the FTC's action against Vision I Properties, LLC, doing business as CartManager International. http://www.ftc.gov/opa/2005/03/cartmanager.htm

Effective oversight of vendors requires processes before, during and after the relationship. Before you send a vendor personal information, the prospective service provider should be examined, qualified and bound by appropriate and detailed contract provisions. During the term, the vendor should be monitored – vendors who process sensitive data should likely be assessed by you or an independent third party. At the end of the term, steps should be taken to ensure that all the personal information has been returned or destroyed.

Attachment 2 to this paper contains some sample contract terms for data processor vendor contracts. These terms may be shared with your legal counsel to provide a checklist for assessing your own standard terms.

If you have any questions or comments about this article or third party data processing standards generally, please do not hesitate to contact Peggy Eisenhauer at 404-914-1163 or via email to peggy@privacystudio.com

ATTACHMENT 1
Standard Elements in FTC Consent Decrees for Privacy/Security Breaches

(Based on an Analysis Of 14 Recent FTC Actions[15])

1. **No misrepresentation.** Company shall not misrepresent the extent to which it maintains and protects the privacy, confidentiality, security, or integrity of any personal information.

2. **Limits on disclosure of personal information to 3rd parties** – if the incident included inappropriate disclosure of personal information**.**

   a) Company shall not disclose to any third party any personal information in violation of its published privacy policy, without first obtaining the express, affirmative (opt-in) consent of the individual to whom such personal information relates.

   b) [if applicable] Company shall not apply material privacy policy changes to information collected from or about individuals before the date of the posting, unless Company obtained the express, affirmative (opt-in) consent of the individuals to whom such personal information relates.

3. **Consumer Education** – if applicable. For 5 years, Company shall place on all websites a clear and conspicuous notice regarding [privacy and security practices].

4. **Security Program.**

   a) Company shall establish and maintain a comprehensive security program reasonably designed for the protection of its collected personally identifiable information. The program shall include:

      (1) Designation of personnel to coordinate and oversee the program;

      (2) Identification of risks to the security, confidentiality and integrity of personal information could result in the unauthorized disclosure or misuse of information, including an assessment of risks related to employee and agents, information systems, and potential system failures;

      (3) Design and implementation of reasonable safeguards to identified risks, including training and proper oversight of employees and agents; and

      (4) Evaluation and adjustment of the security program according to ongoing assessment findings and material changes in business.

   b) Within 180 days after service of order and thereafter biannually for ten (10) years, Company must obtain an assessment and report from an independent, third party that (i) sets forth the specific safeguards implemented and maintained by the Company, (ii) explains how such safeguards are

[15] Compilation of terms contained in the FTC consent decrees with: DSW (December 2005), Superior Mortgage (September 2005), BJ's (June 2005), Ohio Art Co. April 2005), Petco (March 2005), CartManager (March 2005), Gateway Learning (September 2004), Tower Records (June 2004), Bonzi Software (February 2004), Guess (August 2003), Education Research Center Of America (May 2003), Hershey Foods (February 2003), Microsoft (December 2002) and Eli Lilly (May 2002). Copies of all these consent decrees can be found online at www.ftc.gov.

appropriate for the size and complexity of the Company, the nature and scope of the Company's activities and the sensitivity of the information, (iii) explains how the safeguards meet or exceed the protections in item 3 above; and (iv) certifies that the Company's security program is operating with sufficient effectiveness to provide reasonable assurances that consumer information is protected.

5. Maintenance of Relevant Documents and Notification of Changes.

a) For a period of five years, Company shall provide to the FTC (upon request): (1) a copy of each representation made to individuals regarding the collection, use and security of collected information; (2) all plans, reports or other materials relating to the Company's compliance with the order; and (3) any document that contradicts, qualifies or questions, the Company's compliance with the order.

b) For a period of five years, Company must make available to the FTC all documents demonstrating compliance with the order, including: (1) a copy of each different privacy statement or communication with the date, full text, html address, and graphics; (2) a copy of documents seeking to obtain opt-in consent of consumers and any documents demonstrating such consent provided by consumers; (3) all invoices, communications, and records relating to the disclosure of personally identifiable information to third parties.

c) Company shall notify the FTC at least 30 days prior to any corporate change which may affect its compliance with the order.

6. Delivery of Order. Company must delivery a copy of this order to all current and future principals, officers, directors, managers and all employees with managerial responsibility over the subject matter of the order.

7. Duration of the FTC Order with Penalties for Violations.

a) Within 180 days after service of order and thereafter as requested, file a report with the FTC setting forth the Company's compliance with the order.

b) Except as otherwise indicated in the final order, the final order terminates in twenty years. Each violation of the final order may result in a civil penalty of $11,000.

ATTACHMENT 2
Sample Vendor Privacy and Information Security Procedures

Privacy & Information Management Services – Margaret P. Eisenhauer, P.C.
Provided for Reference Purposes Only

Recommended Practice: Develop "Vendor Privacy and Information Security Requirements" which contain privacy and security requirements for vendors that handle personal information for or on behalf of Company. Incorporate this Requirements document into all vendor contracts. Also use this Requirements document in RFP and vendor qualification processes.

The Requirements document should include (i) general privacy and information security obligations, (ii) data collection, creation, use, storage, access and disclosure privacy requirements, (iii) information security requirements, (iv) administrative obligations, and (v) data disposition procedures. The requirements are set forth below. For each of these requirements, the vendor must provide (and Company should confirm) information on the vendor's ability to meet the standards described.

Sample Contract Provisions – please note these are general provisions, provided for informational and reference purpose only. These provisions are NOT appropriate for contracts pursuant to which any volume of sensitive data is transferred. They are also NOT designed to meet legal requirements that apply to the processing of regulated data (such as consumer financial or healthcare data). PLEASE CONSULT YOUR LEGAL COUNSEL BEFORE USING ANY OF THESE PROVISIONS!

1. General Privacy and Information Security Obligations

   a. Vendor will keep strictly confidential all personal information [or use defined term that reflects the specific information to be processed by the vendor] that it obtains, creates or accesses on behalf of, or in connection with any services it provides to or for, Company ("Personal Information").

   b. Vendor will collect, create, use, store, access, disclose and otherwise handle Personal Information only as specifically authorized by, and as necessary to perform authorized services for or on behalf of, Company (the "Authorized Services"). *[tie with services contemplated in the contract]*

   c. Vendor will implement and maintain strict data handling procedures with respect to particularly sensitive Personal Information such as health and financial information. *[or determine what level of proportional protections should be imposed on more sensitive data, such as the consumer reporting data]*

   d. Vendor will use appropriate administrative, technical and physical safeguards to protect the security, confidentiality and integrity of Personal Information in Vendor's custody or control.

2. Data Collection, Creation, Use and Storage

a. Vendor will minimize the amount of Personal Information it collects, creates, uses and stores to that which Vendor genuinely needs to perform the Authorized Services.

b. Vendor will create copies of documents and other media containing Personal Information only as necessary to perform the Authorized Services.

3. Data Access and Disclosure

a. Vendor will limit access to Personal Information, and only disclose Personal Information, to Vendor's employees who need to know the information to perform the Authorized Services.

b. Except as specified below, Vendor will not disclose Personal Information to any third party without the prior written consent of Company.

c. Vendor may disclose Personal Information to other Company vendors and to Vendor's contractors and consultants, but only to the extent such entities or individuals:

- need to know the information to perform the Authorized Services;
- agree to disclose the information to need-to-know employees only; and
- are subject to a confidentiality agreement (in a form approved by Company).

d. Vendor will comply with these requirements in disclosing, transmitting or providing access to Personal Information to any other person or entity.

3. Vendor will disclose to Company employees who request Personal Information only that information which is minimally necessary to fulfill the request. If the requesting individual is not Vendor's primary Company contact, Vendor will promptly notify such contact of the information request and Vendor's response to the request.

4. Information Security Requirements

a. Vendor will develop, implement and maintain a comprehensive written information security program. The program will contain appropriate administrative, technical and physical safeguards to protect the security, confidentiality and integrity of the Personal Information in Vendor's custody or control.

b. Vendor will regularly test or otherwise monitor the effectiveness of the safeguards' controls, systems and procedures. Vendor will periodically identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of the Personal Information, and ensure that there are safeguards in place to control those risks.

5. Administrative Obligations

a. In addition to the information security program described in Section 4, Vendor will develop, implement and maintain privacy policies and procedures that are designed to enable Vendor to comply with these requirements.

b. At appropriate intervals or as otherwise requested by Company, Vendor will provide a copy of its written privacy and information security policies and procedures to (i) Company and (ii) appropriate employees, contractors and consultants of Vendor.

c. Vendor will conduct appropriate background investigations of employees, contractors and consultants, as appropriate No employee, contractor or consultant shall be given access to the Personal Information until such investigation is complete and the results are acceptable.

d. Vendor will conduct privacy and information security training, as appropriate, for its employees, contractors and consultants. The training will be conducted at reasonable intervals to periodically reinforce awareness of privacy and information security issues. Vendor will provide enhanced privacy and information security training to employees, contractors and consultants who interact directly with Company consumers.

e. Vendor will require any employee, contractor or consultant who handles Personal Information to sign a confidentiality agreement (in a form approved by Company).

f. Vendor will monitor all employees, contractors and consultants for compliance with these guidelines.

g. Vendor will promptly and thoroughly investigate allegations of any use or disclosure of Personal Information of which Vendor is aware that is in violation of these guidelines, and will promptly notify Company in writing of any significant violation.

h. Vendor will promptly mitigate, to the extent practicable, any harmful effect of which Vendor is aware of any use or disclosure of Personal Information in violation of these guidelines.

6. Data Disposition

a. At appropriate intervals, unless otherwise provided in a written agreement between Vendor and Company, Vendor will (i) return to Company all documents and other media in Vendor's possession or control containing Personal Information, and (ii) purge, delete or destroy, to the extent reasonably practicable, any Personal Information that cannot feasibly be returned to Company. With respect to identical copies of documents or other media whose originals have been returned to Company, Vendor will purge, delete or destroy such copies.

b. With respect to the disposition of Personal Information, Vendor will follow the instructions provided to it by Company to ensure that the Personal Information is appropriately purged, deleted or destroyed. Vendor shall provide Company with an Officer's Certificate to certify its compliance with these procedures.