CHAPTER 1.

Introduction

1:1. The rise of information security and privacy

Information security and privacy issues are not new, but mass attention and compliance efforts are at an all time high, and appear only to be increasing, particularly as litigation and high-profile security breaches continue to draw attention to these issues. That privacy and information security concerns have been a societal problem for a long time is demonstrated by the fact that many wiretapping laws are called “eavesdropping” laws, referring to people standing in the so-called eavesdrop of a house listening to conversations before telephones were invented.

Current hot issues in information security and privacy include the following:

- pretexting;
- financial privacy;
- privacy litigation;
- outsourcing to foreign countries;
- electronic health records and personal health records; and
- social networking.

Issues that have arrived, but without complete impact on the privacy landscape, include interoperability of medical records, non-HIPAA covered medical information,
genetic privacy, and increased concerns over computer crimes and control of one’s identity. Just a few years ago, there were a limited number of privacy and security laws in the United States, and they generally applied only to companies in certain industries (such as health care and financial institutions). Now, the number of laws is staggering. Many new laws apply, or will apply, to companies in all industries, not just certain industries. Moreover, though there is no federal law that generally requires information security, certain Federal Trade Commission (“FTC”) actions indicate that the FTC is imposing a generalized duty to impose information security via the Federal Trade Commission Act. As this trend continues, many companies may face a situation where data security issues must be directly and quickly addressed, or they will incur extensive FTC-mandated administrative costs and burdens.

Compliance with these laws is not only a legal reality, but it is also a business reality, as frequent and well-publicized data security incidents demonstrate. These days the newspapers are full of stories about high-profile data security incidents that usually involve numerous consumers. This, in large part, results from the 46 states, plus Puerto Rico, New York City, and Washington D.C., that have enacted laws that require notice of security breach incidents. These laws have increased the publicity that is received when these incidents occur, heightening consumer awareness of the incidents. Security breach is now a concern under HIPAA due to the recent changes to HIPAA that should be finalized in 2011, and now many foreign countries are beginning to enact security breach laws as well.

Notice of security breach laws is just one of the categories of laws that are being enacted. Identity theft is also an area of great legislative concern. Numerous states have enacted privacy and security laws that cover a variety of information categories, including the following:

- internet privacy restrictions;
- financial privacy;
- unauthorized access to networks and information;
- wiretapping and privacy in electronic communications;
- identity theft;
- data security and data destruction;
- notice of data security breaches;
- spyware and phishing;
- restrictions upon the use of Social Security numbers;
- video and cable privacy;
- genetic privacy;
- pretexting;
- telecom privacy; and
- restrictions upon government entities.

As this book will demonstrate, these general categories represent just the tip of the regulatory and administrative iceberg. Within these and other categories, there are an extensive number of laws and regulations and myriad issues a company must consider if it intends to comply with these requirements. Moreover, there are laws, including laws
regarding wiretapping, that are becoming more important as electronic communication becomes the preferred mechanism for business communication. Also, contrary to popular belief, many of these privacy and security laws apply to all companies, not just companies in the health or financial industries or those that collect data regarding children.

Now, with more and more companies exploring international markets, the laws of the European Union (“EU”) and other countries are becoming more relevant. These laws differ in many ways from the laws in the United States and compliance with one standard, even the generally higher EU standard, will not guarantee U.S. compliance. Moreover, other nations, including Japan and Argentina, have also enacted broad privacy laws. The laws of these jurisdictions are the subject of *Information Security and Privacy: A Guide to International Law and Compliance* (West 2010).

The cost of failing to comply with these requirements is high. In addition to the regulatory fines and penalties, companies face litigation costs defending suits by individuals, as well as, in some cases, class action suits alleging violations of these laws. The direct costs of remedying non-compliance after an incident can be staggering—some companies have disclosed costs that reach into the millions of dollars. And these costs do not include the potential loss of business that can result from consumer trepidation created by a company permitting the wrongful acquisition of a consumer’s data.

### 1:2. General privacy principles

Laws that regulate privacy and security typically involve restrictions on the collection of data (usually information that identifies a person, particularly if coupled with other sensitive information), the transfer or dissemination of information, and the security of the information, as well as the accuracy of the information that is collected and stored. As the discussion below demonstrates, certain organizations have expressed these principles in different ways, but all of these laws involve the application of these principles.

### 1:3. Organisation for Economic Co-operation and Development Guidelines: a beginning

The Organisation for Economic Co-operation and Development (“OECD”) is a group of 34 member countries, including the United States, that wish to foster democratic government and the market economy. The OECD was one of the first organizations to recognize the issues that privacy could create in a global economy and to generate what was, in essence, a model for member countries to follow regarding privacy practices. This occurred on September 23, 1980, when the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (“OECD Guidelines” or “Guidelines”) were adopted. If there is one document that serves as the basis of the privacy laws that are in existence today, particularly the EU Data Protection Directive, it is the OECD

---

1. See generally, [http://www.oecd.org/document/58/0,2340,en_2649_201185_1889402_1_1_1_1,00.html](http://www.oecd.org/document/58/0,2340,en_2649_201185_1889402_1_1_1_1,00.html) (last visited February 4, 2011).

2. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html](http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html) (last visited February 4, 2011).
Guidelines. While these guidelines are not binding, even on the member countries, they are useful in providing a framework for later privacy legislation.

The OECD Guidelines contain the following principles:

- collection limitation principle;
- data quality principle;
- purpose specification principle;
- security safeguards principle;
- openness principle;
- individual participation principle;
- accountability principle; and
- international application principle.

1:4. Scope of OECD Guidelines

The Guidelines apply to personal data, in both the public and private sectors, which, because of the manner in which it is processed or because of the nature or the context in which it is used, poses a danger to privacy and individual liberties. The Guidelines do not prevent the application of different protective measures to different categories of personal data depending upon the nature and the context in which the data was collected, stored, processed, or disseminated; the exclusion from the application of the Guidelines of personal data that obviously does not contain any risk to privacy and individual liberties; or the application of the Guidelines only to automatic processing of personal data.

Exceptions to the Guidelines, set forth in Sections 2 and 3 of the Guidelines, including those that are related to national sovereignty, national security, and public policy, are intended to be as few as possible and made known to the public. Ultimately, these Guidelines are considered minimum standards, which are supplemented by additional measures for the protection of privacy and individual liberties.

1:5. Collection limitation principle

The OECD Guidelines call for limits to the collection of personal data and requires that any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

---

4. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Part 1, Section (3) (a) to (c).
5. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Part 1, Section 4(a) to (b).
1:6. **Data quality principle**

Personal data should also be relevant to the purposes for which it is to be used, and to the extent necessary for those purposes, should be accurate, complete and up-to-date.\(^8\)

1:7. **Purpose specification principle**

The purpose for which personal data is collected should be specified not later than at the time of data collection. Subsequent use should be limited to the fulfillment of these purposes or others that are not incompatible with these purposes. New purposes must be specified on each occasion of change of purpose.\(^9\) Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with this requirement except with the consent of the data subject, or by the authority of law.\(^10\)

1:8. **Security safeguards principle**

Personal data should be protected by reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure of data.\(^11\)

1:9. **Openness principle**

The Guidelines suggest that there should be a general policy of openness about developments, practices, and policies with respect to personal data. Readily available means should exist to establish the existence and nature of personal data and the main purposes of its use, as well as the identity and usual residence of the data controller.\(^12\)

1:10. **Individual participation principle**

The Guidelines suggest that individuals should have the right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to the individual; to have communicated to him data relating to him within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner, and in a form that is readily intelligible to him; to be given reasons if a request is denied,

---

10. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Part 2, Section 10(a) to (b).
12. “Data controller” means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Part 1, Section 1(a).
and to be able to challenge a denial; and to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.  

1:11. **Accountability principle**

A data controller should be accountable for complying with measures that give effect to these principles.  

1:12. **International application: free flow and legitimate restrictions**

The Guidelines encourage member countries to consider the implications for other member countries of domestic processing and re-export of personal data. Member countries are also encouraged to take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a member country, are uninterrupted and secure. Member countries are cautioned to refrain from restricting transborder flows of personal data between themselves and other member countries except where another country does not substantially observe these Guidelines or where the re-export of such data would circumvent a country’s domestic privacy legislation. A member country may also impose restrictions regarding certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of the data and for which the other member country provides no equivalent protection. Member countries are also encouraged to avoid developing laws, policies, and practices in the name of the protection of privacy and individual liberties that would create obstacles to transborder flows of personal data that would exceed requirements for these protections.

1:13. **National implementation**

In implementing the principles set forth above, member countries are encouraged to establish legal, administrative or other procedures or institutions for the protection of
privacy and individual liberties in respect of personal data. Member countries are particularly encouraged to adopt appropriate domestic legislation; to encourage and support self-regulation, whether in the form of codes of conduct or otherwise; to provide for reasonable means for individuals to exercise their rights; to provide for adequate sanctions and remedies in case of failure to comply with measures that implement these principles; and to ensure that there is no unfair discrimination against data subjects.

1:14. International cooperation

Member countries are also encouraged, where requested, to make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other member countries which comply with these Guidelines. Member countries are also encouraged to establish procedures to facilitate information exchange related to these Guidelines and mutual assistance in the procedural and investigative matters involved.

Member countries are also encouraged to work toward the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

1:15. Principles adopted by the Asia-Pacific Economic Cooperation

The Asia-Pacific Economic Cooperation (“APEC”) is an organization similar to the OECD, but for the Pacific Rim. It too has adopted privacy principles that are supposed to serve as the basis for legislation for member countries: the APEC Privacy Framework 2004 (“Framework”). As with the OECD guidelines, the Framework provides high-level principles that do not provide significant detail regarding legislation, but do provide a direction for member countries.

As a general matter, exceptions to the principles contained in the Framework, including those relating to national sovereignty, national security, public safety, and public policy, should be limited and proportional to meeting the objectives to which the exceptions relate, and should be made known to the public to the extent permitted by local law.

22. Id. (a) to (e).
24. Id.
1:16. APEC information privacy principles

Preventing Harm

Personal information protection should be designed to prevent the misuse of information, in light of the interests of the individual to legitimate expectations of privacy. Specific obligations should factor in this risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use, and transfer of personal information.

Notice

Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include the fact that personal information is being collected; the purposes for which personal information is collected; the types of persons or organizations to whom personal information might be disclosed; the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information; and the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.

Additionally, all reasonably practicable steps should be taken to ensure that notice is provided either before or at the time of collection of personal information. Otherwise, notice should be provided as soon after as is practicable. It should be noted that under the Framework, it may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information.

Collection Limitation

The collection of personal information should be limited to information that is relevant to the purpose for which it is collected. The information should be proportional and collected through lawful and fair means, and, if appropriate, with notice given to the individual.

31. APEC Privacy Framework 2004, Principle II, Section 15(a) to (e).
33. Id.
34. APEC Privacy Framework 2004, Principle II, Section 17.
36. Id.
Chapter 1: Introduction

**Uses of Personal Information**

Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except with the consent of the individual whose personal information is collected; when necessary to provide a service or product requested by the individual; or by the authority of law and other legal instruments, proclamations, and pronouncements of legal effect.  

**Choice**

Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible, and affordable mechanisms to exercise choice in relation to the collection, use, and disclosure of their personal information. It may not be appropriate for personal information controllers to provide choice when collecting publicly available information.

**Integrity of Personal Information**

Personal information should be accurate, complete, and up-to-date to the extent necessary for the purposes of use.

**Security Safeguards**

Personal information controllers are to protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification, or disclosure of information or other misuses. The safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.

**Access and Correction**

The APEC Framework suggests that individuals should be able to obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them; have communicated to them, after having provided sufficient proof of their identity, personal information about them within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner, in a form that is generally understandable; and challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended, or deleted. Access and opportunity for correction should be provided except where the burden or expense of doing so would be unreasonable or disproportionate.

---

39. Id.
42. Id.
43. APEC Privacy Framework 2004, Principle VIII, Section 23(a) to (c).
to the risks to the individual’s privacy in the case in question; the information should not be disclosed due to legal or security reasons or to protect confidential commercial information;\(^{44}\) or the information privacy of persons other than the individual would be violated.\(^{45}\) If a request or a challenge is denied, the individual should be provided with reasons why and be able to challenge the denial.\(^{46}\)

**Accountability**

A personal information controller should be accountable for complying with measures that give effect to these principles.\(^ {47}\) When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these principles.\(^ {48}\)

### 1:17. Privacy and security: the seven U.S. privacy principles

In the United States, the principles are expressed slightly differently, but also in a form that is non-binding on many companies. There are a variety of state and federal privacy statutes that identify different duties and obligations regarding the level of privacy afforded to consumers’ information. As a general principle, the differences relate to the type of information in question and the type of business involved, as well as what jurisdiction the consumer resides in. U.S. laws reflect these privacy principles in different ways.\(^ {49}\)

Following are the seven U.S. privacy principles:

**Notice.** Companies can be required to give individuals notice about the purpose for which private information was gathered, as well as how information collected by a company will be used. A company can also be required to provide users with information regarding how they can register complaints and inquire regarding privacy issues, whether a company discloses information to third parties, and what the methods and standards are for limiting and using information.

**Choice.** Companies can be required to give users the option of not disclosing their personal information to a third party and requesting that their information not be utilized for purposes other than those originally disclosed at the time of collection. For certain sensitive information, companies must receive explicit permission from the user before the information is disclosed to third parties or used for purposes other than that for which it was originally collected.

---

44. “Confidential commercial information” is information that an organization has taken steps to protect from disclosure, where such disclosure would facilitate a competitor in the market to use or exploit the information against the business interest of the organization causing significant financial loss.


46. *Id.*


48. *Id.*

49. These principles have been expressed in the EU Safe Harbor principles, which are not applicable to many U.S.-based businesses. They represent general principles regarding privacy that are reflected to varying degrees in different federal and state laws.
Chapter 1: Introduction

Onward Transfer. Before a company discloses any information to a third party, it can be required to apply the above-referenced notice and choice principles. If a third party is acting as an agent for a company, the third party in some circumstances can be required to comply with the privacy principles as well.

Access. Companies typically are required to permit users to have access to their personal information. A company can also be required to afford users the opportunity to amend, delete, or alter personal information when it is inaccurate, with the caveat that access need not be provided when the cost of providing access would be disproportionate compared to the risk of violation of the individual’s privacy or when providing access would violate another’s privacy.

Security. A bedrock principle of many privacy laws is information security. While absolute security is not required, a company can be required to take reasonable precautions to protect private information from misuse, disclosure, unauthorized access or alteration, particularly if affirmative representations regarding data security are made.

Data Integrity. Ensuring the accuracy and completeness of the data can also be required. One of the main principles is that private information collected by a company must be relevant to the purposes for which it was collected.

Enforcement. Companies can also be required to provide some enforcement mechanism to protect an individual’s privacy rights, including a reasonably affordable and accessible dispute-resolution system. They can also be obligated to self-remedy problems arising out of their failure to meet the requirements of the principles.