Chapter 1

Introduction

KeyCite®: Cases and other legal materials listed in KeyCite Scope can be researched through the KeyCite service on Westlaw®. Use KeyCite to check citations for form, parallel references, prior and later history, and comprehensive citator information, including citations to other decisions and secondary materials.

§ 1:1 The rise of data privacy and security

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. Now, the number of laws is staggering. Moreover, though there is no federal law that generally requires information security, certain Federal Trade Commission actions indicate that the

FTC is, for the first time, imposing a generalized duty to impose information security via the Federal Trade Commission Act. If this trend continues many companies may face a situation where data security issues must be directly and quickly addressed, or they will face 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 the frequent and well publicized data security incidents demonstrate. These days the newspapers are full of stories about the high-profile data security incidents that usually involve numerous consumers. This in large part results from the over 35 states that have enacted laws that require notice of security breach incidents. These laws have increased the publicity that is received when these incidents occur and heighten consumer awareness of incidents.

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

- General 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;
- Internet privacy;
- Telecom privacy; and
- Restrictions upon government entities.

As this book demonstrates, these general categories represent just the beginning of the regulatory and administrative hurdles. Within these, and other categories, there are an extensive number of laws and regulations that must be complied with and considered if a company intends upon complying with these requirements. Moreover, there are laws, including laws regarding wiretapping, that are becom-

ing more important as electronic communications become the norm for business communication. Also, contrary to popular belief, many of these laws apply to all companies, not just companies in the health or financial industries, or companies that collect data regarding children.

Now, with more and more companies exploring international markets, the laws of the European Union and other counties 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 several EU countries, as well as countries such as Japan and Argentina are also covered in this book.

Privacy is also becoming a business reality as more consumers are paying attention to privacy issues and security breaches. Consumers are not alone. There are an ever-increasing number of privacy laws that are being enacted at the state level. Moreover, the federal government has become increasingly active on the privacy front, as the new federal laws that are in this edition of this book demonstrate.

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, 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 30 member countries, including the United States, that wish to foster democratic government and the market economy.[1] The OECD was one of the first organizations to recognize the issues that privacy could create in a global economy and to generate a 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 were adopted. If there is one document that served as the basis of the privacy laws that are in existence today, particularly the EU Data Directive, it is the OECD Guidelines. While these guidelines are not binding, even on the member countries, they are useful in providing a framework for later privacy legislation. The principles in the OECD guidelines are the: Collection limitation principle; Data quality principle; Purpose specification principle; Security safeguards principle; Openness principle; Individual participation principle; Accountability principle; and International application principles.

§ 1:4 Scope of OECD Guidelines

The Guidelines apply to personal data,[1] in both the public or 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.[2] The Guidelines do not prevent the application to different categories of personal data, of different protective measures

---

[Section 1:3]

[1]See, generally, http://www.oecd.org/document/58/0,2340,en__2649__201185__1889402__1__1__1__1,00.html (last visited February 17, 2007).

[Section 1:4]

[1]"Personal data" means any information relating to an identified or identifiable individual (data subject). Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 1, Section 1(b).

[2]Part 1, Section 2.

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 which obviously does not contain any risk to privacy and individual liberties; or the application of the Guidelines only to automatic processing of personal data.[3]

Exceptions to the Guidelines in Sections 2 and 3, including those that are related to national sovereignty, national security and public policy were to be as few as possible and made known to the public.[4] Ultimately, these Guidelines were to be considered minimum standards which were to be supplemented by additional measures for the protection of privacy and individual liberties.[5]

§ 1:5 Collection limitation principle

The OECD Guidelines call for limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.[1]

§ 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 kept up-to-date.[1]

§ 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 and the subsequent use limited to the fulfillment of these purposes or others that are not incompatible with those purposes and

---

[3]Part 1, Section (3)(a) to (c).

[4]Part 1, Section 4(a) to (b).

[5]Part 1, Section 6.

[Section 1:5]

[1]Part 2, Section 7.

[Section 1:6]

[1]Part 2, Section 8.

as are specified on each occasion of change of purpose.[1] 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.[2]

§ 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.[1]

§ 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[1].

§ 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 him; 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; be given reasons if a request is

---

[Section 1:7]

[1]Part 2, Section 9.

[2]Part 2, Section 10(a) to (b).

[Section 1:8]

[1]Part 2, Section 11.

[Section 1:9]

[1]"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 Persona Data, Part 1, Section 1(a).

Part 2, Section 12.

denied, and to be able to challenge a denial; and challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.[1]

§ 1:11 Accountability principle

A data controller should be accountable for complying with measures which give effect to these principles.[1]

§ 1:12 International application: Free flow and legitimate restrictions

The Guidelines also encourage Member countries to consider the implications for other Member countries of domestic processing and re-export of personal data.[1] Member countries were also encouraged to take all reasonable and appropriate steps to ensure that transborder flows of personal data,[2] including transit through a Member country, are uninterrupted and secure.[3] A Member country was also cautioned to refrain from restricting transborder flows of personal data between itself and another Member country except where the other country does not substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation.[4] 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.[5]

Member countries were also encouraged to avoid develop-

[Section 1:10]

[1]Part 2, Section 13(a) to (d).

[Section 1:11]

[1]Part 2, Section 14.

[Section 1:12]

[1]Part 3, Section 15.

[2]"Transborder flows of personal data" means movements of personal data across national borders. Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 1, Section 1(c).

[3]Part 3, Section 16.

[4]Part 3, Section 17.

[5]Part 3, Section 17.

ing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for these protections.[6]

§ 1:13 National implementation

In implementing the principles set forth in above, Member countries were encouraged to establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data.[1] Member countries were particularly encouraged to: adopt appropriate domestic legislation; encourage and support self-regulation, whether in the form of codes of conduct or otherwise; provide for reasonable means for individuals to exercise their rights; provide for adequate sanctions and remedies in case of failures to comply with measures which implement these principles; and ensure that there is no unfair discrimination against data subjects.[2]

§ 1:14 International cooperation

Member countries were also encouraged, where requested, to make known to other Member countries details of the observance of the principles set forth in these Guidelines.[1] 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.[2] Member countries were also encouraged to establish procedures to facilitate information exchange related to these Guidelines, and mutual assistance in the procedural and investigative matters involved.[3]

Member countries were also encouraged to work towards

---

[6]Part 3, Section 18.

[Section 1:13]

[1]Part 4, Section 19.

[2]Part 4, Section 19(a) to (e).

[Section 1:14]

[1]Part 5, Section 20.

[2]Part 5, Section 20.

[3]Part 5, Section 21.

the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.[4]

§ 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. As with the OECD guidelines, these are high-level principles that do not provide significant detail regarding legislation, but certain provide a direction for member countries. These Principles are contained in a Framework that was adopted in 2004.

As a general matter, exceptions to these 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 made known to the public, or in accordance with law.

§ 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.[1] 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.[2]

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

---

[4]Part 5, Section 22.

[Section 1:16]

[1]Part III, Principle I, Section 14.

[2]Principle I, Section 14.

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.[3]

Additionally, all reasonably practicable steps were to be taken to ensure that notice is provided either before or at the time of collection of personal information.[4] Otherwise, notice should be provided as soon after as is practicable.[5] It should be noted that under the Guidelines, it may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information.[6]

Collection Limitation

The collection of personal information should be limited to information that is relevant to the purpose for which it is collected.[7] The information should be proportional and collected through lawful and fair means, and, if appropriate, with notice given to the individual.[8]

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.[9]

Choice

Where appropriate, individuals should be provided with

---

[3]Principle II, Section 15(a) to (e).

[4]Principle II, Section 16.

[5]Principle II, Section 16.

[6]Principle II, Section 17.

[7]Principle III, Section 18.

[8]Principle III, Section 18.

[9]Principle IV, Section 19.

clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information.[10] It may not be appropriate for personal information controllers to provide choice when collecting publicly available information.[11]

Integrity of Personal Information

Personal information should be accurate, complete and kept up-to date to the extent necessary for the purposes of use.[12]

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.[13] 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.[14]

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.[15] Access and opportunity for correction should be provided except where:

---

[10]Principle V, Section 20.

[11]Principle V, Section 20.

[12]Principle VI, Section 21.

[13]Principle VII, Section 22.

[14]Principle VII, Section 22.

[15]Principle VIII, Section 23(a) to (c).

the burden or expense of doing so would be unreasonable or disproportionate 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;[16] or the information privacy of persons other than the individual would be violated.[17] If a request or a challenge is denied, the individual should be provided with reasons why and be able to challenge the denial.[18]

Accountability

A personal information controller should be accountable for complying with measures that give effect to these Principles.[19] 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.[20]

§ 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 principal the differences relate to the type of information in question, the type of business involved, as well as what jurisdiction the consumer resides in. All of these laws in essence address the privacy principles in different

---

[16]"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.

[17]Principle VIII, Section 24.

[18]Principle VIII, Section 24.

[19]Principle IX, Section 25.

[20]Principle IX, Section 25.

ways.[1]

These seven U.S. privacy principles are:

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.

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 to provide access would violate another's privacy.

Security. A bedrock principle of many privacy laws is information security. While absolute security is not required, a

---

[Section 1:17]

[1]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 and not all of these have been adopted or codified by U.S. law at this time. The EU Safe Harbor is discussed in Chapter 26.

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 principals 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 its failure to meet the requirements of the principles.