Contents

Preface .................................................. ix
Peter P. Swire, CIPP/US, Kenesa Ahmad, CIPP/US

Acknowledgments .................................... xi
Richard Soule, CIPP/E

Introduction .......................................... xiii
J. Trevor Hughes, CIPP

CHAPTER ONE
U.S. Legal Framework
  Branches of the Government .......................... 1
  Sources of Law in the United States ....................... 2
  Key Definitions .................................................. 5
  Regulatory Authorities ............................................ 7
  Self-regulation .................................................... 7
  Understanding Laws ............................................. 7
  Conclusion ......................................................... 9

CHAPTER TWO
Federal and State Regulators and Enforcement of Privacy
  Types of Litigation and Enforcement ......................... 11
  Federal Privacy Enforcement and Policy Outside of the FTC ......................... 12
  FTC Jurisdiction .................................................. 14
  FTC Enforcement Process and Consent Decrees ......................... 15
  Privacy Policies and Notices, Early FTC Enforcement Actions and Deceptive Trade Practices ......................... 16
  Enforcement Actions and Unfair Trade Practices ......................... 18
  Federal 2012 Privacy Reports and the Future of Federal Enforcement ......................... 20
  State Enforcement .................................................. 22
  Self-regulation and Enforcement ......................... 23
  Cross-border Enforcement Issues ......................... 24
  Conclusion ......................................................... 26
CHAPTER THREE
Global Information Management from a U.S. Perspective

- The Role of the Privacy Professional .................................................. 29
- Risks of Using PI Improperly ................................................................. 30
- Developing an Information Management Program .............................. 31
- Data Sharing and Transfer ................................................................. 33
- Privacy Policies and Disclosure ......................................................... 36
- Managing User Preferences and Access Requests ............................. 38
- Contract and Vendor Management ..................................................... 41
- Conclusion ......................................................................................... 43

CHAPTER FOUR
Medical Privacy: HIPAA and GINA

- The Health Insurance Portability and Accountability Act of 1996 .......... 46
- The Health Information Technology for Economic and Clinical Health Act ................................................................. 51
- Genetic Information Nondiscrimination Act of 2008 .......................... 52
- Conclusion ......................................................................................... 54

CHAPTER FIVE
Financial Privacy

- The Fair Credit Reporting Act ............................................................ 57
- The Fair and Accurate Credit Transactions Act .................................. 64
- Gramm-Leach-Bliley Act ...................................................................... 66
- Dodd-Frank Wall Street Reform and Consumer Protection Act ........... 71
- Required Disclosure Under Anti-Money-Laundering Laws ................. 72
- Conclusion ......................................................................................... 74

CHAPTER SIX
Education Records

- An Overview of FERPA ....................................................................... 77
- FERPA and the Protection of Pupil Rights Amendment .................... 81
- Conclusion ......................................................................................... 82

CHAPTER SEVEN
Telecommunications and Marketing

- Regulations Governing Telemarketing .............................................. 85
- Fax Marketing ...................................................................................... 95
- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ................................................................. 96
- The Telecommunications Act of 1996 .............................................. 100
- The Cable Television Privacy Act of 1984 ....................................... 101
- The Video Privacy Protection Act of 1988 ....................................... 102
CHAPTER EIGHT
Privacy Statutes About Online Activities
  The Children’s Online Privacy Protection Act of 1998 .................................................. 107
  California’s Online Privacy Protection Act ................................................................. 111
  Conclusion ...................................................................................................................... 112

CHAPTER NINE
Information Security and Data Breach Notification Laws
  Information Security ..................................................................................................... 116
  Data Breach Notification .............................................................................................. 117
  Fundamentals of Incident Management ....................................................................... 118
  State Breach Notification Laws ..................................................................................... 119
  State Data Destruction Laws ......................................................................................... 125
  Conclusion ...................................................................................................................... 126

CHAPTER TEN
Privacy Issues in Investigations and Litigation
  Disclosures Required, Permitted or Forbidden by Law .................................................. 130
  Privacy and Civil Litigation ............................................................................................ 133
  Law Enforcement and the Role of Privacy Professionals .............................................. 138
  National Security and the Role of Privacy Professionals .............................................. 145
  Conclusion ...................................................................................................................... 149

CHAPTER ELEVEN
Workplace Privacy
  Legal Overview ............................................................................................................ 153
  Privacy Issues Before, During and After Employment ................................................... 158
  Conclusion ...................................................................................................................... 175

Index ................................................................................................................................ 181

About the Authors ............................................................................................................. 193

Figure List
  Table 1-1. Three Branches of U.S. Government .......................................................... 1
  Figure 3-1. Steps for Information Management ......................................................... 31
  Figure 3-2. Sample Organization Chart for Privacy and Data Protection Activities........ 32
T
he first two chapters discussed the U.S. legal framework and legal privacy concepts. This chapter will focus on privacy management policies. Privacy and information management in most organizations require a combination of skills, including legal skills but also often expertise in marketing, sales, human resources, public and government relations and information technology. In large organizations, privacy professionals may be part of a team that draws on a mix of these skill sets.

This chapter begins by examining some major benefits and risks of using personal information (PI) in the private sector. Next, it discusses best practices for developing an information management program that addresses privacy and other information management concerns, including security. A related task is to perform a data inventory of an organization’s data storage and transfers, and to achieve benefits and mitigate risks based on the results of that inventory.

The chapter then turns to management issues connected to the prominent fair information practices of notice, choice and access, and concludes with a discussion of contract and vendor management.

This material should be read in the context of more detailed discussions of legal rules in the other chapters of this book. The important information management issues associated with data breach and incident response are examined in Chapter 9. Considerable discussion of information security issues is provided in Chapter 4 of *Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws and Practices*.

1. The Role of the Privacy Professional

Privacy professionals need to appreciate both the benefits and the risks of using personal information. PI is essential to most businesses—every organization with employees or even volunteers manages PI. Organizations may collect consumer PI for many purposes, both directly from prospective and existing customers and indirectly through enhanced data available from public and private sources. Organizations may disclose information to service providers, affiliates,
business partners and government agencies for a wide range of purposes. At the same time, as discussed in this book and Chapter 1 of Foundations of Information Privacy and Data Protection, many risks can arise from the collection, use and disclosure of PI.

Perceptions of acceptable privacy practices vary, creating challenges for privacy professionals. Decades of opinion surveys show that substantial parts of the population fit within three groups: the “privacy concerned” (people with a strong desire to protect privacy), the “privacy unconcerned” (people with low worries about privacy) and the “privacy pragmatists” (people whose concern about privacy varies with context and who are willing to give up some privacy in exchange for benefits).¹ Perceptions about privacy risks not only vary within the population, they also shift over time. Sometimes the shift is toward greater privacy protection. For example, Social Security numbers used to be visible through the envelope window of millions of Social Security and Supplemental Security Income checks mailed by the U.S. Treasury. With rising fears of identity theft, that practice was abolished in 2000.² Sometimes the shift is toward less privacy protection. For example, people post intimate details of their lives on widely adopted social networks.

Established standards exist for information security, such as installing firewalls or using industry-standard encryption for communications. For many privacy issues, there is less consensus about good practice. Laws vary across jurisdictions and industry sectors, and views about good practice often differ, both within an organization and in the general public. One role for privacy professionals is to alert their organizations to these often divergent perspectives.

Privacy professionals also help their organizations manage a range of risks that can arise from processing personal information, and do so in a manner consistent with meeting the organization’s growth, profitability and other goals. Privacy professionals can help the organization to identify areas where compliance is difficult in practice, and design policies to close gaps between stated policies and actual operations.

2. Risks of Using PI Improperly

Four types of risks must always be considered and balanced.

1. **Legal risks.** The organization must comply with applicable laws—state, federal and international—regarding its use of information or potentially face litigation or regulatory sanctions such as lengthy consent decrees. The company must also comply with its contractual commitments, privacy promises and some industry standards, such as the Payment Card Institute Data Security Standard.

2. **Reputational risks.** Organizations can face legal enforcement and reputational harm if they announce privacy policies but do not carry them out. An organization should seek to protect its reputation as a trusted institution with respected brands.

3. **Operational risks.** Organizations must also ensure that the privacy program is administratively efficient and cost-effective. If a privacy program is too heavy-handed, it may interfere with relationships and inhibit use of PI in ways that would benefit the organization and your customers, such as for personalization or risk management.
4. **Investment risks.** The organization must be able to receive an appropriate return on its investments in information, information technology and information processing programs, in light of evolving privacy regulations, enforcement and expectations.

3. **Developing an Information Management Program**

Over time, PI management has become vital to a large range of organizations. It is now increasingly common for companies to develop an information management program, to seek a holistic approach to the risks and benefits of processing PI. The program, in turn, helps create policies and practices for important parts of the organization’s activities. Common activities for such policies include maintaining preference lists for direct marketing, developing appropriate security for human resources data, executing proper contracts to authorize international data flows and publishing online privacy notices when data is collected.

In creating the information management program, privacy leaders help their organizations develop privacy policy in an organized way, meeting policy goals as well as preserving business flexibility. Privacy professionals seek to understand and anticipate future changes both in the regulatory environment and in their companies’ business needs. To achieve these objectives, companies should take four distinct steps.

3.1 **Four Basic Steps for Information Management**

Figure 3-1 summarizes the four steps—discover, build, communicate and evolve—followed by a closer look at each phase.

Figure 3-1. Steps for Information Management

<table>
<thead>
<tr>
<th>1</th>
<th>Discover</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Build</td>
</tr>
<tr>
<td>3</td>
<td>Communicate</td>
</tr>
<tr>
<td>4</td>
<td>Evolve</td>
</tr>
</tbody>
</table>

- **Discover**
  - Issue identification and self-assessment
  - Determination of best practices

- **Build**
  - Procedure development and verification
  - Full implementation

- **Communicate**
  - Documentation
  - Education

- **Evolve**
  - Affirmation and monitoring
  - Adaptation
3.1.1 Phase 1: Discover

Before drafting or updating a privacy policy, consider the company’s environment, information goals and corporate culture. What laws regulate the company’s collection or use of information? Does the company wish to be aggressive in its use of information? Does the company instead plan to be more cautious in its use of PI, to reduce legal and reputational risks or perhaps to achieve a competitive advantage as a privacy-sensitive leader? How do the company’s information policy objectives mesh with those of its competitors, customers and business partners? The answers to these questions can help an organization define its information policy goals. These goals serve as the foundation upon which the company’s policies are built.

In addition to the many state, federal and international laws that regulate the collection, use and/or disclosure of personal information, many industry groups have promulgated self-regulatory guidelines. Some of these standards are mandatory for members of the specific industry group, as discussed in Chapter 2.

Useful privacy guidance for an organization depends on an accurate understanding of the company’s actual data practices, as well as its intended data use. The successful privacy professional forges honest and open relationships with individuals across departments and at different levels in the organization’s hierarchy. The participation of a range of departments, including legal compliance, customer service, marketing, IT, human resources and sales, is often beneficial in the creation of an information plan. The team should have the knowledge base and influence in the organization to determine and articulate the company’s current practices and future goals.

Figure 3-2. Sample Organization Chart for Privacy and Data Protection Activities
3.1.2 Phase 2: Build

Armed with an accurate assessment of the organization’s practices and goals, the privacy professional can help determine how best to meet those goals, by both facilitating and restricting flows of PI where appropriate. Successful building of the information management program requires close coordination between those writing the policies (whose expertise may include legal compliance and protection of reputation) and those who actually operate consistent with the policies.

3.1.3 Phase 3: Communicate

Along with developing and implementing the information management program, the organization must assure effective communication to internal and external audiences. Internal audiences must be trained on policies and procedures, with individual accountability for compliance. Specific policies and more general goals should be communicated clearly to the organization’s decision makers and consumer-facing employees, so they can shape appropriate messages to relevant audiences.

Transparency is also critical. A written privacy notice must accurately reflect the company’s practices. As discussed further below, companies over time have increasingly used a layered privacy notice approach—placing a summary form that highlights key terms of the policy on top of a longer, more detailed statement of privacy and security practices.

3.1.4 Phase 4: Evolve

Information uses constantly evolve in response to changing technology, laws, market conditions and other factors. Once an information management program is established, there must be a process for review and update.

4. Data Sharing and Transfer

This section examines practices and controls for managing PI in the often complex flows among U.S. business enterprises, both within the United States and across geographic boundaries, and addresses data inventory, data classification, documenting data flows and determining data accountability.

4.1 Data Inventory

It is important for organizations to undertake an inventory of the PI that it collects, stores, uses or discloses—whether within the organization or to outside entities. This inventory should include both customer and employee data records. It should document data location and flow as well as evaluate how, when and with whom the organization shares such information—and the means for data transfer used.

This sort of inventory is legally required for some institutions, such as those covered by the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, discussed in Chapter 5. The benefits of the inventory apply more generally, by identifying risks that could affect reputation or legal
compliance. If a problem subsequently occurs, penalties are likely to be less severe if the company has an established system of recording and organizing this inventory. The inventory should be reviewed and updated on a regular basis.

4.2 Data Classification
After completing an inventory, the next step is to classify data according to its level of sensitivity. The data classification level defines the clearance of individuals who can access or handle that data, as well as the baseline level of protection that is appropriate for that data.

More sensitive data generally requires greater protection than other information, and may be segregated from less sensitive data, such as through access controls that enable only authorized individuals to retrieve the data, or even kept in an entirely separate system. By contrast, if all data is held in the same system, then temporary or lower-level employees might gain access to sensitive data. Holding all data in one system can increase the consequences from a single breach.

Most organizations handle different types of PI, such as personnel and customer records, along with other information the organizations treats as sensitive, such as trade secrets and business plans. In the United States, classification is often important for compliance purposes because of sector-specific privacy and security laws. As discussed throughout this book, different rules apply to financial services information, medical information and numerous other categories. An effective data classification system helps an organization address compliance audits for a particular type of data, respond to legal discovery requests without producing more information than necessary, and use storage resources in a cost-effective manner.

4.3 Documenting Data Flows
Once data has been inventoried and classified, its data flows should be examined and documented. An organization chart can be useful to help map and document the systems, applications and processes handling data. Documenting data flows helps identify areas for compliance attention.

4.4 Determining Data Accountability
Privacy professionals often have significant responsibility within an organization to assure compliance with privacy laws and policies. Here are some helpful questions for privacy professionals when doing due diligence and for an organization to consider as it addresses privacy risks:

- **Where, how and for what length of time is the data stored?**
  Data breach laws have focused increasing attention on where and how an organization stores PI. The organization needs policies to address potential risks of data lost from laptops as well as centralized computer centers.

- **How sensitive is the information?**
  As discussed above, data should be classified according to its level of sensitivity. Though the data management cycle includes many participants—from the data owner to the
privacy professional, the information security professional, the vendor (if applicable), the auditor (if applicable) and the end user—ultimately, the data owner is responsible for assigning the appropriate sensitivity level, or classification, to the information based on company policy. Common categories include confidential, proprietary (e.g., property of the organization), sensitive, restricted (e.g., available to select few) and public (e.g., generally available).

- **Should the information be encrypted?**
  Under many breach notification laws, no notice is required if the lost PI is encrypted or protected by some other effective technical protection. Such laws have encouraged greater use of encryption for stored data, and security good practices have included a wider use of encryption over time. On the other hand, encryption can be difficult to implement correctly and may reduce function in some applications. IT professionals should be consulted about how to take advantage of encryption while achieving other organization goals.

- **Will the information be transferred to or from other countries, and if so, how will it be transferred?**
  Because different countries have significantly different privacy laws, an organization should familiarize itself with the privacy requirements of both origination and destination countries for trans-border data flows.

- **Who determines the rules that apply to the information?**
  U.S. privacy professionals have increasingly used some terms that are included in the EU Data Protection Directive—for example, a “controller” is an entity who “determines the purposes and means of the processing of personal data” and a “processor” is an entity that “processes personal data on behalf of the controller.” Privacy professionals should assess which organization determines the rules that apply to the processing of data. If an organization stores data on behalf of another, the organization should expect to be required to meet the privacy policy guarantees of the other entity (the controller) in the use and storage of such data. Most likely, a storing company (or processor) will be required to sign a contract to this effect.

- **How is the information to be processed, and how will these processes be maintained?**
  The processes through which personal information is processed also must be defined. Steps should be taken to train staff members involved in the processes, and computers on which the information will be processed should be secured appropriately to minimize the risk of any data leak or breach. Physical transfer of the data also should be secured.

- **Is the use of such data dependent upon other systems?**
  If the use of personal data depends on the working condition of other systems, such as specialized computer programs, the condition of those systems must also be evaluated and updated if necessary. A system that is outdated may call for developing a new method or program for using the relevant data.
5. Privacy Policies and Disclosure

Privacy policies are central to information management programs. They inform relevant employees about how PI must be handled, and in some cases are made public in the form of a privacy notice for the purpose of transparency. As discussed in the previous chapter on enforcement, they also are important as legal documents. If an organization violates a promise made in a privacy policy that is also communicated in the privacy notice, then the FTC or state attorney general may bring an enforcement action for a deceptive practice.

Statements on a company website are often called either “privacy notices” or “privacy policies.” This book uses the term privacy policy when referring to the internal organization statement of policies, designed to communicate to those inside the organization what practices to follow, and privacy notice for external communications. In practice, however, “privacy policy” is often used to refer to statements made for both external and internal audiences.

5.1 One or Multiple Privacy Policies

An organization must determine whether to have one privacy policy that applies globally to all of its activities, or multiple policies. One policy makes sense if an organization has a consistent set of values and practices for all its operations. Multiple policies may make sense for a company that has well-defined divisions of lines of business, especially if each division uses customer data in very different ways, does not typically share PI with other divisions and is perceived in the marketplace as a different business.

Sometimes separate corporations decide to use a common privacy policy. For financial holding companies, the same corporate name may be used by multiple subsidiaries and affiliates, and a single privacy policy can avoid confusion about how PI will be handled. More specifically, mutual funds and their advisors are separate corporations, but may decide to adopt a joint privacy policy and a joint form of notice. All of the mutual funds in a corporate “family” may use joint notices.

Conversely, using multiple policies can create complications. One division’s privacy policy may be more stringent in a particular way than another division’s, preventing sharing of customer information between two parts of the same company. Where multiple policies are used, it makes sense to align policies as closely as possible so as not to hinder cooperation between divisions.

5.2 Policy Review and Approval

An organization should not finalize a privacy policy without legal consultation followed by executive approval. If the policy is not strict enough, then consumers, regulators and the press may criticize the company for its failure to protect privacy. If a policy is too strict, then open-ended statements or overly ambitious security promises can result in legal penalties or reputational problems if the promises are not met.

If a privacy policy is revised, the organization should announce the change first to employees, then to both current and former customers in the form of a notice. In a 2012 report, the FTC
stated that companies should obtain express affirmative consent (opt-in) before making material retroactive changes to privacy representations. The FTC stated that a “material” change “at a minimum includes sharing consumer information with third parties after committing at the time of collection not to share the data would constitute a material change.”

5.3 Communication of Privacy Policy Through a Notice

The content of privacy notices is based on fair information practices such as the OECD Guidelines and Asia-Pacific Economic Cooperation (APEC) Principles. It is generally easy to see the privacy notices of competitors, other organizations or your own organization by going to the relevant websites. Communication to consumers and other external stakeholders may use multiple methods:

1. **Make the notice accessible in places of business.** Clearly post the organization’s privacy notice at the location of business in areas of high customer traffic and in legible form. Organization staff also should have ready access to copies of the up-to-date company privacy policy in case a customer wishes to obtain a copy for review.

2. **Make the notice accessible online.** The websites of most organizations, even those primarily involved in offline commerce, today contain the privacy notice. It is standard to have a link from the company’s front page.

3. **Provide updates and revisions.** For financial institutions, GLBA requires that customers receive the privacy notice annually, with clear notice of the customer’s right with respect to opt-outs. For institutions without this sort of required updating, provide good notice when the privacy policy is revised, with express customer consent for material changes and a clear opportunity to opt out for smaller changes.

4. **Ensure that the appropriate personnel are knowledgeable about the policy.** Organization staff who interact with PI should receive training in the organization’s privacy policy. HIPAA creates specific training requirements for all employees of covered entities. Especially for employees working with sensitive data, organizations should provide regular training and keep records of which employees have been trained.

As one type of appropriate training, customer service representatives (CSRs), such as in customer call centers, should receive a summary statement or script that describes the privacy notice and can be used to answer customer questions. CSRs should have a full copy of the privacy notice in their standard reference material and should retain the ability to send or direct customers to a copy of the privacy notice that they can review in detail. They should know how to escalate privacy issues or incidents once observed.

5.4 Policy Version Control

An organization’s privacy policy will need to be updated as information collection, use and transfer needs evolve. As such changes occur, a new version of the privacy policy must be drafted to replace the older version. Replacement of the policy must occur systematically across all areas of posting (physical and electronic) to reduce the risk that representations made under different
versions of the policy will be implemented. Privacy policies should reflect the policy revision date along with a version number, if used.

For compliance purposes, it is useful to save and store older versions of the privacy policy and its associated notice. These earlier versions may be useful internally, such as to show what representations have been made in connection with which customer transactions. The earlier versions may also be useful in the event of an enforcement action, to reduce the risk that the company will be held to an incorrect set of representations.

6. Managing User Preferences and Access Requests

In following their privacy policies, organizations can face management challenges on topics including how to manage user (data subject) preferences and respond to requests for access and correction. Legal rules may set basic requirements for what must be done, but privacy professionals must often choose options within those requirements, and ensure that implementation occurs correctly. The discussion here illustrates major areas where user preferences are handled through opt-in, opt-out or no option, and then examines management issues for handling user preferences and customer access and redress requests.

6.1 Opt-in, Opt-out and No Option

Privacy professionals should become aware of situations that call for different approaches to user preferences, notably an opt-in (also called “affirmative” or “express” consent), an opt-out or no option for the consumer.

Some U.S. privacy laws require affirmative consumer consent, or opt-in, before data is used or collected. For instance, COPPA requires express consent from a parent before a child’s PI is collected. HIPAA requires opt-in consent before personal health information is disclosed to third parties, subject to important exceptions. The Fair Credit Reporting Act requires opt-in before a consumer’s credit report may be provided to an employer, lender, or other authorized recipient. As discussed above, the FTC believes that opt-in consent should occur before PI collected under one privacy notice is processed under a materially changed privacy notice.

Some industry segments commonly employ opt-in, such as for e-mail marketers who send a confirmation e-mail requiring a response from the subscriber before the subscriber receives actual marketing e-mails. This e-mail approach is sometimes called “double opt-in” or “confirmed opt-in,” because a consumer first indicates interest in the mailing list and then confirms that interest in response to the follow-up e-mail. In addition, the EU takes a general position that opt-in consent is the appropriate way for marketing to occur, and this position was underscored in the draft Data Protection Regulation issued in early 2012.

On the other extreme, no consumer choice, or no option, is expected in a range of situations. The 2010 preliminary FTC staff report, Protecting Consumer Privacy in an Era of Rapid Change, called these situations “commonly accepted practices.” For example, a consumer who orders a product online expects her PI to be shared with the shipping company, the credit card processor and others who are engaged in fulfilling the transactions. The consumer does not
expect to have to sign an opt-in or be offered an opt-out option for the shipping company to learn the address. In addition to product fulfillment, other examples provided by the FTC include “internal operations such as improving services offered, fraud prevention, legal compliance and first-party marketing” by the seller to the customer. The FTC received public comments that the term “commonly accepted practices” would not work well for companies providing innovative services. The final report, in 2012, addressed the same issue by saying: “Companies do not need to provide choice before collecting and using consumers’ data for practices that are consistent with the context of the transaction, consistent with the company’s relationship with the consumer, or as required or specifically authorized by law.”

It is common practice for companies to offer an opt-out, sometimes referred to as consumer choice, before customer information is sold or shared with third parties. This privacy notice creates an enforceable promise. If an individual sells the information for individuals who have opted out, the FTC or state enforcers may bring suit under the unfair and deceptive trade practices laws.

Some U.S. statutes require that a company provide at least an opt-out. For example, GLBA requires an opt-out before transferring the PI of a customer of a financial institution to an unaffiliated third party for its own use. The Video Privacy Protection Act requires an opt-out before covered movie and other rental data is provided to a third party. The CAN-SPAM Act requires email marketers to provide an opt-out. The Do Not Call rules provide the opportunity to opt out of telemarketing phone calls, both in general or on a company-by-company basis.

Opt-outs are required for companies who subscribe to any of a number of self-regulatory systems. For instance, the Direct Marketing Association has long operated an opt-out system for consumers who do not wish to receive commercial mail sent to their homes. The Network Advertising Initiative and Digital Advertising Alliance operate opt-out systems in connection with online advertising.

### 6.2 Managing User Preferences

Effective management of user preferences can become quite challenging, especially for organizations that interact with their customers with multiple channels and for multiple products. The following are some of these challenges.

1. The **scope** of an opt-out or other user preference can vary. As mentioned above, financial institutions must provide an opt-out by law prior to sharing personal information with third parties, but sharing with affiliates can be done without offering such an opt-out. An organization must decide how broadly an opt-out or other user preference will apply. Some opt-out rules are by channel, such as specific limits on phone calls or commercial e-mails.

2. The **mechanism** for providing an opt-out or other user preference can also vary. A good rule of thumb is that the channel for marketing should be the channel for exercising a user preference. This rule is written into law for the CAN-SPAM Act, where an e-mail solicitation must be exercisable by the consumer through an online mechanism; it is not acceptable under the law to require the customer to mail or call in their opt-out. Similarly, if communication with a customer is done via a website, good
practice is to enable user preferences to be expressed through a web channel, and not to insist on mailing or a phone call.

3. **Linking** of a user’s interactions can be a management challenge when customers interact with an organization through multiple channels, including in person, by phone (phone number), by e-mail (e-mail address) or by web. Good practice is for the organization to implement the opt-out or other user preference across channels and platforms. Under GLBA a bank receiving an opt-out request from a customer must comply across all communications regardless of the media used to communicate the request.

4. The **time period** for implementing user preferences is sometimes provided by law. For instance, the CAN-SPAM Act and Telemarketing Sales Rules mandate specific time periods for processing customer preferences.

5. **Third-party vendors** often process PI on behalf of the company that has the customer relationship. In such instances, the user preferences expressed to the first organization should be honored by the vendor.

### 6.3 Customer Access and Redress

Some U.S. laws provide consumers with clear rights to access the PI held about them. For instance, individuals have the right to access their credit reports under the Fair Credit Reporting Act, and rectify incorrect data. Patients can access their medical records under HIPAA, with records that the patient believes are incorrect noted as such in the patient files. Where customer access is not required under a specific statute, access is included in statements of fair information practices such as the OECD Guidelines and the APEC Principles, and in the U.S.–EU Safe Harbor agreement and the EU Data Protection Directive. The 2012 White House and FTC reports also place increased emphasis on a general consumer right to access with respect to data held in the commercial sector.

A good baseline to determine when access requests should be granted is the APEC Principles, which provide guidance on the proper scope of access requests and appropriate exceptions to providing access:\textsuperscript{13}

Individuals should be able to:

a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them;

b) have communicated to them, after having provided sufficient proof of their identity, personal information about them;

i. within a reasonable time;

ii. at a charge, if any, that is not excessive;

iii. in a reasonable manner; and, 

iv. in a form that is generally understandable;

c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.
Such access and opportunity for correction should be provided except where:

i. the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual’s privacy;

ii. the information should not be disclosed due to legal, security or commercial proprietary reasons; or,

iii. the information privacy of persons other than the individual would be violated.

If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial.

7. Contract and Vendor Management

Many U.S. organizations elect to outsource information processing to an outside vendor or plan to sell the collected information to a third party. Specific precautions must be taken if a company plans to share personal data with a third-party data processor.

7.1 Vendor Contracts

Companies are responsible for the actions of vendors they contract with to collect, analyze, catalog or otherwise provide data management services on the company’s behalf. The claims in a privacy policy also apply to third parties when they are working with an organization’s data. To ensure the responsibility and security of data once it is in the hands of a contractor or vendor, precautions to consider incorporating in written contracts include:

1. **Confidentiality provision.** Contractors and vendors involved in personal information collection for an organization—or with whom an organization shares data—should be required to sign a contract containing a confidentiality provision before engaging in business that uses the information.

2. **No further use of shared information.** The contract with the vendor managing personal information on the organization’s behalf should specify that the data be used only for the purposes contracted.

3. **Use of subcontractors.** If the vendor intends to use subcontractors in the collection or use of personal information, the contractor organization should require that all subcontractors follow the privacy and security protection terms in the vendor’s contract (which, in turn, should be consistent with the organization’s own privacy protection terms). Vendor contracts should also address whether the data can flow across borders to ensure that the organization’s policy on this issue is not violated.

4. **Requirement to notify and to disclose breach.** An organization should require prompt notification in the event of a data breach or breach of contract. Details of the breach should be disclosed promptly and in detail.

5. **Information security provisions.** Contracts may include provisions concerning specific security controls; encryption of data in transit, on media and on portable
devices; network security; access controls; segregation of data; employee background checks; audit rights and so on.

7.2 Vendor Due Diligence

A procuring organization may have specific standards and processes for vendor selection. A prospective vendor should be evaluated against these standards. Standards for selecting vendors may include:

1. **Reputation.** A vendor’s reputation with other companies can be a valuable gauge of the vendor’s appropriate collection and use of personal data. Requesting and contacting references can help determine a vendor’s reputation.

2. **Financial condition and insurance.** The vendor’s finances should be reviewed to ensure the vendor has sufficient resources in the case of a security breach and subsequent litigation. A current and sufficient insurance policy can also protect the procuring organization in the event of breach.

3. **Information security controls.** A service provider should have sufficient security controls in place to ensure the data is not lost or stolen. Further discussion of these controls is contained in *Foundations of Information Privacy and Data Protection*.

4. **Point of transfer.** The point of transfer between the procuring organization and the vendor is a potential security vulnerability. Mechanisms of secure transfer should be developed and maintained.

5. **Disposal of information.** Appropriate destruction of data and/or information in any format or media is a key component of information management—for both the contracting organization and its vendors. As discussed in Chapter 5, the Disposal Rule under the Fair and Accurate Credit Transactions Act of 2003 sets forth required disposal protections for financial institutions. The Disposal Rule requirements provide a good baseline for disposal of PI more generally.

6. **Employee training and user awareness.** The vendor should have an established system to train its employees about its responsibilities in managing personal or sensitive information.

7. **Vendor incident response.** Because of the potentially significant costs associated with a data breach, the vendor should clearly explain in advance its provisions for responding to any such breach.
8. Conclusion

Effective information management addresses legal and reputation risks while using information appropriately to meet the organization’s goals. Protection of privacy requires far more than writing policies that comply with applicable law; actual implementation must occur within the fast-paced and demanding setting of modern business. By designing and implementing a good information management program, privacy professionals can play a vital role in helping their company achieve both business success and good privacy practices.

Endnotes

7 45 C.F.R. § 164.530(b)(1).
10 www.dmachoice.org/dma/static/about_dma.jsp.
11 www.networkadvertising.org/managing/opt_out.asp.
12 www.aboutads.info/choices/.