Foundations of Information Privacy and Data Protection

A Survey of Global Concepts, Laws and Practices

Peter P. Swire, CIPP/US
Kenesa Ahmad, CIPP/US
Managing Editor
Terry McQuay, CIPP/US, CIPP/C, CIPP/E, CIPP/G

An IAPP Publication
Contents

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

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

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

CHAPTER ONE
Common Principles and Approaches to Information Privacy and Data Protection
  Defining Privacy .................................................. 1
  Classes of Privacy .................................................. 2
  The Historical and Social Origins of Privacy ...................... 2
  Information Privacy, Data Protection and the Advent of Information Technology ......................... 4
  Personal and Nonpersonal Information ......................... 4
  Sources of Personal Information .................................. 7
  Processing Personal Information ................................. 8
  Human Resources, Customers and Other Categories of Personal Information ......................... 9
  Privacy Policy and Notice Defined. .............................. 11
  Information Risk Management ..................................... 12
  Fair Information Practices ....................................... 15
  Privacy or Data Protection Officers and Offices ............... 23
  Summary .............................................................. 25
CHAPTER FIVE
Online Privacy: Using Personal Information on Websites and Other Internet Technologies

Overview of Web Technologies ......................................................... 115
Privacy Considerations for Online Information .................................. 119
Summary ....................................................................................... 142

INDEX .............................................................................................. 145

ABOUT THE AUTHORS ................................................................. 155

List of Figures
Figure 1-1: Responsible Management Processes for Data Privacy Compliance ............................................. 24
Figure 4-1: Privacy vs. Security ............................................................................. 78
Figure 4-2: Life Cycle of Incident Management ............................................................................. 104
Figure 5-1: Short Privacy Notice ............................................................................. 122
Figure 5-2: Web Form Soliciting User Information ............................................................................. 127
Figure 5-3: False Security Warning ............................................................................. 133
Figure 5-4: Cookie Prompt in Microsoft Internet Explorer .......................................................... 135
CHAPTER THREE

Sectors of Privacy
and Data Protection Law

Not all types of personal information are created equal. Going back generations, there have been special confidentiality rules for certain types of sensitive data, including medical and financial data. As practitioners learn about modern privacy and data protection rules, they should be aware that additional and specialized rules may apply in these sensitive areas. This chapter discusses important sectors of privacy and data protection, notably medical confidentiality; financial privacy; telecommunication laws; online activity regulations; and rules that apply to governments, human resource management, smart grid and smart home issues, and direct marketing.

1. Healthcare Sector

Special privacy protections for healthcare date back thousands of years. The modern Hippocratic oath states, “I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know.”¹ The concept of doctor-patient confidentiality exists in many countries as a matter of both tradition and law. Many countries also have specific healthcare privacy laws that they have enacted over time. The Health Insurance Portability and Accountability Act (HIPAA) is a prominent example of the sector-specific approach the United States takes towards privacy. Under the EU Data Protection Directive, healthcare is also singled out as “sensitive” data. Article 8 of the Directive specifically provides that member states can impose stricter rules for health-related information. Provinces in Canada and other countries also have specific healthcare laws providing for stringent privacy protection. Accordingly, privacy practitioners who encounter healthcare information during the course of their work should be alert to the possibility that special rules may apply.

There are several reasons why strict privacy and data protection laws are necessary for healthcare privacy information. First, at the most basic level, medical information is related to the inner workings of one’s body or mind. One’s individual sense of self may be violated if others have unfettered access to this information. Second, most doctors believe that patients will be
foundations of information privacy and data protection

more open about their medical conditions if patients have assurance that embarrassing medical facts will not be revealed. Third, medical privacy protections can protect employees from the risk of unequal treatment by employers. For instance, a person who has had an abortion, contracted a sexually transmitted disease or had psychiatric treatment could potentially be fired if a prejudiced employer gained access to this information. In countries where the employer pays for health insurance, companies may have financial incentives to avoid employing workers who suffer from expensive medical conditions or who may be at higher risk of expensive conditions based on their genetic background.

Despite the existence of strict laws protecting medical information, modern medical practice often uses patient medical information quite intensively. For example, information about medical procedures is frequently used to assure accurate payment for those services. Doctors in one location may wish to access records about a patient’s medical treatment in other cities in order to treat the patient appropriately. Researchers also use medical information, sometimes de-identified, in trying to find new patterns as they seek to develop cures for illnesses and promote public health.

2. Financial Sector

Banking and other financial records have long been treated with high levels of confidentiality. Medieval and early modern banks often kept the identity of their borrowers secret and would not reveal intimate financial details of their customers. One reason for this confidentiality was to encourage borrowers to report honestly to the lender about their other debts and ability to pay. Another priority in the financial sector is to assure security—thieves and fraudsters can target individuals or transactions if they have access to these details.

Today, many countries use sector-specific rules both to protect the privacy of financial information and to ensure that information is appropriately shared with the government and other related players. In the United States, the Gramm–Leach–Bliley Act of 1999 established a complicated set of privacy and security requirements for all financial institutions.2 In Japan, the Act on the Protection of Personal Information and accompanying guidelines regulate the use of customers’ personal information in the financial services sector.3 Also, many countries have historically used “bank secrecy” laws, which prohibit banks from turning over details about their customers, especially to authorities in other countries who are seeking to enforce tax or other laws. Switzerland is famous for its bank secrecy laws; however, those rules have relaxed over time. Today, various “offshore” jurisdictions carry on extensive financial activities and continue to use bank secrecy laws.

Recently, enforcement against money laundering has resulted in greater government access to financial records, both within each nation and internationally. The global focus on fighting terrorism has accelerated the spread of money-laundering laws with the goal of preventing or detecting flows of funds to international terrorists. Major country economies have also put pressure on the offshore countries to reveal financial records, as a way to both fight terrorism and enforce their tax laws.

Privacy and security experts in the financial system, therefore, must remain aware of the requirements for both confidentiality and disclosure. Specialized financial rules can apply
either to financial institutions or to financial transactions, and differ depending on the type of institution or transaction. For example, security measures for banks are often subject to different rules and the scrutiny of different oversight agencies than other institutions because of the higher risk of theft and the need for oversight by bank regulators. Money-laundering laws apply to many organizations, from casinos to car dealers, to encourage government reporting on suspicious financial activities. In addition, rules vary from country to country for reporting on an individual’s credit history. Privacy professionals should thus be alert for the possibility of special local rules for information about credit histories.

3. Telecommunications Sector

Telecommunication privacy rules historically applied to wiretaps and other access to telephone activities. Increasingly, telecommunication privacy rules apply to other forms of communication such as e-mail, chat or web surfing. It is easiest to understand the range of modern telecommunications rules by distinguishing three categories. First, wiretaps and similar technologies gain access to the content of the communication, such as what people say on the telephone or write in a chat or e-mail. Second is access on an ongoing basis to to/from information, identifying each phone number or e-mail address contacted by an individual. Third, stored telecommunication records can reveal both content (what an e-mail said last month) and contact information (who sent or received an e-mail or a call to the person last month).

Telecommunication information is highly prized by law enforcement and national security agencies. The to-from information can aid police in identifying possible accomplices or coconspirators. The content of the information, such as that retrieved from a telephone wiretap, can reveal the precise plans and activities of a criminal suspect. Because these records have the potential to be very useful for law enforcement agencies, but are also extremely personal, many countries have passed specific wiretap and related laws to protect the privacy of these communications. These laws typically set standards and establish procedures for government access to the communications. These same laws usually make it a crime for private citizens to wiretap or gain unauthorized access to this information. Additionally, electronic communication and other usage records, such as lists of e-mails sent or phone calls made, are typically subject to specific laws that limit access by nongovernmental actors. To understand the privacy concerns about telecommunications, imagine that your employer or family members could listen to every phone call you made. This form of invasive surveillance could easily chill your willingness to speak openly with the person on the other end of the line.

With the rapid adoption and widespread use of mobile devices in recent years, a fourth category of privacy-sensitive information is becoming increasingly important—location information. For the first time in history, people in their everyday lives are carrying a device that reports constantly on their whereabouts. Because widespread use of mobile phones and smartphones is so recent, current debates revolve around who should have access to location information and on what terms.

The growing diversity of telecommunications is accompanied by an increasing range of sector-specific laws and best practice regimes for telephones, e-mails and other forms of
communication. The usefulness of location information to the police, marketers and other actors will also continue to foster complex rules about how to provide appropriate access to information while ensuring privacy and security.

4. Online Privacy

The development of the Internet in the 1990s triggered an ongoing international debate about Internet privacy that continues today. On the one hand, special rules for the Internet violate the principle of technology neutrality, which is the concept that citizens’ rights should not vary depending on a specific technology. On the other hand, the Internet has created new and considerable challenges to privacy protection. First, many Internet privacy problems seem novel, without easy comparisons to past practice. Today a doctor is still a doctor, and a bank is still a bank, but it is hard to know which historical privacy and data protection rules best apply to Internet activity. Second, the Internet enables far more detailed collection of information than has historically been the case. In the offline world, a newspaper would at most possess knowledge of its customers’ names, addresses and subscriptions. On the Internet, by contrast, the newspaper might know exactly which articles were read by which subscribers, providing far more detailed clues as to its users’ preferences. This enormous increase in detail is a great aid to companies that wish to personalize their offerings and provide customers with tailored services and product options. This increased detail, however, also raises privacy concerns, especially because many web users do not possess the technological sophistication to understand exactly how their data is being accessed and used.

The third and perhaps most important way in which the Internet differs is its inherently global nature. Historically, individuals made purchases in person, in their hometown or by mail order. With the Internet, however, a single website can sell goods to customers all around the world. The global nature of the Internet greatly increases the likelihood that the privacy and data protection laws of more than one nation may apply to online transactions. As discussed further in Chapter 5, these issues are important to the ongoing discussion and debate about what online privacy rules should exist.

5. Public Sector

Many nations have different requirements and handling procedures for information held by the government than for information held by corporations and other private actors. For example, the EU Data Protection Directive applies to personal information held by both the government and the private sector. Nonetheless, there are different and generally less strict legal rules for “first pillar” government organizations, where the police and other government agencies hold personal information, than for data held by private actors. In the United States, the Privacy Act of 1974 requires federal agencies to apply fair information privacy practices. Canada has three levels of privacy law: federal, province or territory, and municipality.
There are strong reasons supporting both sides of the debate about whether the government should receive more or less access to private information. Reasons supporting broad government access and use include national security and law enforcement, to protect the basic foundations of society. Governments across the world also administer a wide range of social welfare activities such as healthcare, pensions and education. To run those government programs efficiently, managers often need access to a wide array of personal information.

However, there are also important reasons for concern regarding government access and use of personal information. These problems are easiest to see in totalitarian regimes, where state control is nearly absolute and the individual has no right to privacy. One well-known example is that of the Nazis in Germany, who compiled detailed records about assets held by Jewish citizens. The Nazis later used those records to identify and locate Jews in their mass extermination efforts. Even open and democratic societies have a history of using strong legal protections to limit government invasion of privacy. The Fourth Amendment to the U.S. Constitution generally requires proof of probable cause for a crime before a judge will issue a search warrant or wiretap order. Similarly, Article 8 of the EU Convention on Human Rights provides strong privacy rights against illegal searches and other government intrusions. These limits on government surveillance are often justified as a way to prevent governments from becoming too strong, thereby preventing a potential slide toward abuse of power.

As with the other categories of data information in this chapter, privacy and security practitioners should take special notice when a local or national government has access to personal information. The applicable rules and best practices will often differ from those for similar uses of data by the private sector.

Countries also vary dramatically in their definitions of “public record.” In Sweden, a person’s salary is considered a public record—thus, you can easily access your neighbor’s annual income. In the United States, the owner of real estate is a public record, while that is considered private information in many other countries. In general, it is lawful to access and use information that is available publicly in the home country, such as the American landowner or the Swedish employee. But privacy practitioners should be aware that these rules about “public records” vary from country to country.

6. Human Resources

There is a very long tradition of privacy in human resources (HR) data management. Even before the establishment of data protection laws, HR professionals often kept personnel files locked and separate from other organization records. This is because HR professionals routinely handle personal, sometimes sensitive, information, including nationally issued identification numbers, home address and phone numbers, financial information, criminal record checks and medical information. HR professionals often have access to this information even for the most senior management in the firm. Thus, employers and HR professionals have strong incentive to provide robust privacy protection against misuse and unauthorized disclosure.
Confidentiality issues with employee information begin at the application stage, continue during employment and persist even after termination. When job seekers apply to an available position, they may not wish their current employers or coworkers to know they are seeking a new position. Accordingly, HR professionals must handle application information with discretion. If the position is not outside, but within the applicant’s current place of employment, HR professionals must ensure the confidentiality of salary and other terms of employment, and limit access to assessment of the candidate. Once a person is hired, HR professionals have access to sensitive information, such as financial information and medical information about the employee or family members, including requests for sick leave. Many organizations also conduct annual reviews of employees, and to ensure candor of those involved, privacy measures must be in place. Finally, when an employee leaves an organization, HR professionals must transfer and retain information using the same care as when the employee worked for the organization.

In short, there are numerous reasons to use discretion and confidentiality in the handling of employee files. The widespread adoption of data protection laws has affected the way HR information is treated. HR information is now considered personal data under the EU Directive and the laws of many other countries. This means that employee information must receive the full set of safeguards that apply to other personal information. By contrast, in the United States and many other countries, there is no omnibus privacy protection for such information. Instead, professional organizations such as the International Association for Human Resource Information Management provide a general code of conduct that all members are bound to. HR professionals in the United States must consider the specific privacy obligations under certain privacy sector laws, such as HIPAA and the Fair Credit Reporting Act, both of which require sensitive information to be handled in a way that preserves privacy. States also have a range of laws that protect employee privacy. In addition to outside regulation, most organizations implement internal privacy procedures that establish administrative, technical and physical security of data.

Organizations with employees stationed in more than one country should also be sensitive to the different jurisdictional rules that apply to employee information. For instance, Germany, Austria and other countries with active works councils and trade unions hold certain rights with respect to processing of personal information, including the right to be notified or consulted before an employer introduces measures that may impact the privacy of employees. Further, collective bargaining agreements may address activities that impact the privacy of employees, such as criminal record checks or drug and alcohol testing. Special rules and protections may also apply for government employees, including civil service regimes that are designed to reduce political interference with government employees.

As in other areas of privacy, individuals in countries that follow the EU approach often have a broader range of legal safeguards than individuals in the United States. For example, workplace computer systems in the U.S. are owned and operated by the employer. Individuals, therefore, do not generally have legal rights to use workplace computers free from the company’s supervision. In the EU, by contrast, several countries have ruled that employee e-mail is not subject to unfettered employer access. This is just one example of how the human rights approach in the EU operates in practice and differs from the policies in the United States.
Changes in technology and the work environment raise new privacy issues. The increase in outsourcing of HR functions means that significant amounts of data are being transferred to third parties and other countries. As a result, the risk of potential data security breaches is increased. However, formal vendor security protocols, as well as strict contractual provisions, can help mitigate this risk. The use of strong encryption in data transfer and storage, as well as enhanced loss notification, is now common in vendor negotiation and contracting. Continued technological changes lead to the need for updating and reevaluation of workplace privacy guidelines. The privacy rights of employees in the workplace, in the end, are balanced against legitimate interests of the organization and customers.

7. Smart Grid and Smart Home
The “smart grid” is a recent example of technological innovation that may create privacy issues. The term smart grid refers to a new energy system that manages electricity consumption through remote computerization and automation. The traditional electric transmission system required physically sending workers into the field to read customer meters and find where problems existed in the grid. This traditional system raised few privacy problems, because customer information was gathered only at specific time intervals, such as once a month. With the advent of computerized smart grid services, however, electricity service providers, users, or third-party service providers can now continuously monitor and control the use of electricity to each home or business from a remote location. The new system directly benefits consumers, by providing them with granular control and choice over the extent of their energy consumption. The system itself also operates more smoothly, because managers can detect problems and reroute transmission in the event of natural disasters or other interruptions, improve efficiency and quality of electricity delivery, and link energy sources.

Many nations are investing heavily in smart grid technology and adopting regulations to address accompanying privacy concerns. For example, in 2011 Canada released a report entitled “Operationalizing Privacy by Design: The Ontario Smart Grid Case Study,” which provides guidance for utilities to build privacy into smart grid technology by way of “Privacy by Design.” In the U.S., states are beginning to pass smart grid privacy laws that govern the use and disclosure of data and personal information by utility companies and third parties. Notably, in 2010 California passed a first-in-the-nation consumer protection law regulating use of consumer energy information. In 2011, the EU adopted “Communication Smart Grids: from Innovation to Deployment,” policy directions focused on developing technical standards and ensuring data protection for consumers. Also in 2011, the EU issued an Article 29 Working Party Opinion that clarifies the legal framework applying to smart meters.

This innovative technology, however, also raises new privacy issues regarding consumer personal information. Smart readers measure energy use continuously, rather than at the end of each billing cycle. The information derived from this data collection is personal in that it is easily linked to individuals and families, who may object to potentially invasive behavioral monitoring. For example, this information might allow a malicious hacker to accurately guess when a residence is empty or occupied.
The smart grid, in turn, is an early example of what will likely become the “smart home,” as a growing array of devices helps consumers remotely monitor and control their daily activities. For instance, a refrigerator might report which food is fresh or in low supply, triggering an order to a grocery store. Motion detectors could provide information about who is in the home, allowing parents to remotely monitor the safety of their children. With the extensive ability to collect and use this sort of detailed information, security issues become paramount. Remote hackers could control the smart home and potentially access a massive amount of revealing and sensitive information. The issues for today’s smart grid thus become a template for ongoing privacy and security concerns that will result from the shift to a smart home.

8. Direct Marketing

Direct marketing occurs when the seller directly contacts an individual, in contrast to marketing through mass media such as television or radio. Traditionally, there are two major privacy issues related to direct marketing: what information is collected and used by default, and what rights individuals have to change that default. The first issue concerns which records should be public and the limits on a company’s internal use or resale of targeting information. The second issue includes opt-out measures taken by an individual to limit advertising (“please don’t call my home any more”) or opt-in measures to gain further information (“I do want to receive information about possible discounts on your product”).

Direct marketing developments in the United States have allowed marketers access to a relatively wide range of public records. For instance, in the U.S., a person’s name, address and telephone number are typically available through phone books and registered voter lists. The price of a family’s home is usually available through real estate records. By contrast, most other countries have less extensive sets of public records.

Magazine subscription lists were an early, prominent example of direct marketing. Individuals who subscribed to one magazine (such as a fashion or sports magazine) would receive mail soliciting them to subscribe to similar magazines (other fashion or sports magazines). Over time, a self-regulatory system evolved in the United States, led primarily by the Direct Marketing Association, which established an opt-out system for consumers receiving mailings.10 The next wave of direct marketing involved telephone calls to households. In the United States, a combination of self-regulation and government rules resulted in a company-by-company opt-out list that individuals could join. This expanded in 2004 with implementation of the National Do Not Call Registry, a regulation enforced by the Federal Trade Commission (FTC). By registering, individuals can opt out of receiving telemarketing phone calls. The Do Not Call rule contains an exception for political activities and nonprofit organizations, in order to uphold free speech rights.

With the rise of the Internet, policymakers engaged in extensive debate about how to both enable direct marketing and protect privacy. Enabling marketing was viewed as important in part to support the wide range of free content offered on the Internet. However, privacy concerns continued to surface as websites and companies with an Internet presence received and sometimes used detailed information about user surfing habits.
In 2000, a high-profile court case brought this matter to light. A leading online advertising network, DoubleClick, proposed to combine offline data about users with information collected by cookies set by DoubleClick’s own network. DoubleClick eventually agreed not to merge offline and online data. The decision also prompted the development of a self-regulatory code managed by the Network Advertising Initiative (NAI). The NAI code, for entities that adopt it, requires online advertising networks to provide an opt-out for many forms of online targeted advertising.

With the continued spread of cookies and other online tracking mechanisms, marketing companies increased their use of targeted advertising to Internet and mobile users. These changes have led to new debates about protecting consumer privacy while supporting the Internet economy. The 2002 Privacy and Electronic Communications Directive (e-Privacy Directive) affirmed the right of individuals to place limits on direct marketing in the European Union. The e-Privacy Directive was then amended in 2009. Sometimes called the “Cookie Directive,” its revision placed stricter limits on online advertising than existed before. Notably, it requires affirmative consent before cookies can be placed on an individual’s computer. As of early 2012, national laws implementing the e-Privacy Directive are beginning to come into effect. There have been ongoing discussions about how to comply with the Directive while maintaining functionality of websites that use cookies.

In the United States, recent debates about targeted online advertising have focused mainly on the Do Not Track proposal by the FTC. Proponents of the measure support Do Not Track as a commonsense update to the Do Not Call approach for telemarketing. It is unclear, however, how “tracking” is defined and what sorts of limits should be placed on advertising efforts. The Worldwide Web Consortium (W3C) is establishing standards to define Do Not Track, which may provide guidance on these issues. Beyond the technical issues about how standards should be defined, another controversy surrounds the extent to which Do Not Track would limit only use—the display of targeted ads to those who opt out—or, by contrast, would also limit the collection of information by websites and ad networks.

At a broad level, current issues about direct marketing illustrate the shift from historical broadcast-style marketing to a far more personalized advertising experience. Traditional television ads and billboards were designed for a wide audience, and advertisers received limited feedback about which advertising efforts were effective. Today, however, there is an increasing range of methods that advertisers can use to access information about potential consumers and, in turn, tailor their ads to individual consumer behavior. This personalization both provides individuals with more relevant advertising and affords advertisers a more efficient method of marketing. On the other hand, with personalization also come unprecedented amounts of information that can potentially be linked to the individual, raising privacy concerns. Ongoing changes in technology, such as the rapidly evolving smartphones and mobile marketing ecosystem, will continue to raise controversy and debate about how direct marketing will proceed, consistent with privacy protections.
9. Summary

This chapter has highlighted the possibility that specialized privacy rules and practices can apply to specific sectors, such as healthcare, finance, telecommunications, the Internet and the government. Privacy professionals should be alert to the possible existence of these specialized regimes. Other areas that may have specific rules include human resources, the energy market and marketing (such as limits on phone calls, e-mails, or direct mailings). The basic structure of fair information practices typically applies across these sectors, but the detailed rules and practices may vary.

Endnotes

4  Between 1993 and 2009 the European Union was composed of three legal pillars. The European Community served as the first pillar, the Common Foreign and Security Policy as the second pillar, and the Cooperation in Justice and Home Affairs as the third pillar.
10  Since 1971, the Direct Marketing Association has offered DMAchoice (formerly known as the Mail Preference Service, or MPS), the official mail preference suppression service for the catalog marketing community. See www.dmacheoice.org/.