1

Overview of U.S. Information Privacy Law

The starting point for any discussion of U.S. privacy law must be this simple observation: There is no comprehensive law of privacy in this country. Congress has not passed any statute that sets overall parameters for the handling of personal information by companies in all or even most circumstances. Likewise, the states have not enacted uniform privacy laws; for privacy, there is nothing approximating, say, the Uniform Commercial Code. Nor is there any prospect of uniform, comprehensive federal or state privacy laws being enacted in the foreseeable future. Rather, U.S. privacy law is found—one might say it must be hunted and gathered—from a variety of sources:

- Specific federal statutory guidance on privacy does exist for certain sectors of the economy and types of information (notably healthcare and financial services) and for certain types of consumers (notably children under thirteen). This "sectoral" approach is often contrasted to the approach taken in Europe, where comprehensive privacy laws do exist.

- There are also a handful of specific, prescriptive state laws in the privacy space—for example, California's online privacy laws and Massachusetts' data security laws. Beginning January 1, 2020, the California Consumer Privacy Act takes effect, governing the collection, use, and sale of consumer data by nearly all large and medium-sized companies with any presence in California. Once the CCPA goes into effect, it is likely to become the most comprehensive such regime in the United States.
- Beyond that, companies must look to state and federal laws of general applicability—that is, laws that do not necessarily even mention words like "privacy," but that have been applied to companies' privacy practices. Most importantly, there are both federal and state laws that generally make it illegal to engage in any unfair or deceptive practices. The unfairness prong can be applied to corporate privacy practices that are substantively harmful, while the deception prong can be applied to privacy practices that depart from a company's stated practices.
- Government agencies like the U.S. Federal Trade Commission (FTC) and the California attorney general also regularly issue statements and reports of their views on best practices for privacy. For example, the FTC has called on companies to engage in "privacy by design"—that is, to build privacy protections into their business practices at every stage of development. The FTC likewise has promoted the concepts of disclosure and choice as core elements of a privacy program. While best-practices pronouncements like these do not have the force of law, they can be quite important—especially when issued by an agency like the FTC that has enforcement authority. Such agencies may refer to their own stated views on best practices when considering, in the context of a particular enforcement investigation, whether a company has acted in compliance with the law.

- Self-regulatory privacy codes adopted by industry groups can be important sources of guidance too, as can certification processes offered by private firms. Among other benefits, these are a way of showing consumers, regulators, legislators, and enforcement agencies that industry is both sensitive to privacy issues and capable of keeping its own house clean, without the benefit of additional laws or regulations.

The Basics

Definitions

Q 1.1 What is information privacy law?

"Information privacy" refers to an individual's right to control his or her personal information held by others. Information privacy law refers primarily to the statutes, regulations, and court decisions that guide how organizations may collect or use personal information and what rights or notices they must afford to individuals regarding the use of their personal information.

Q 1.1.1 What types of information do information privacy laws protect?

Information privacy laws typically are aimed at defining personally identifiable information (PII) and protecting such information against nonconsensual use or disclosure. Broadly speaking, PII is information about individuals that discloses their real-world identities to others, that relates to private or sensitive details of their lives, and that they generally would find troubling to have disclosed or used without their knowledge or consent.

Q 1.2 How does information privacy law define "personally identifiable information"?

PII is an ever-evolving concept without a single uniform legal definition. Various laws, regulations, and judicial decisions have defined PII differently, depending on the context.[1] At a minimum, PII includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number). Depending on the legal context, for information to be considered PII, it may be necessary that more than one data element be present (for example, both name and Social Security number).

Some privacy advocates have argued for broader definitions of PII—contending, for example, that because facially anonymous Internet usage data potentially can be connected back to identifiable users, the anonymous data should be treated as PII. For the most part, this broader approach has not yet found a foothold in U.S. law, but more expansive definitions are becoming more popular. For example, the EU's General Data Privacy Regulation and the California Consumer Privacy Act apply a definition of PII that includes essentially any information that could, under some circumstance, identify an individual.

Under some laws and regulations, PII does not include publicly available information—that is, information that is lawfully made available to the general public via federal, state, and local government records.[2]

Q 1.3 What is "sensitive information"?

Like personally identifiable information, "sensitive information" has no single legal definition. Generally speaking, sensitive information can be defined as a subset of PII—consisting of those types of PII that, if disclosed, would be especially troubling to the individuals whose information was exposed. Examples include medical and health information, precise geolocation data (particularly when obtained or used in unexpected ways), personal information of minors, and financial information such as credit card numbers, bank account numbers, and personal income. When it comes to the collection, use, or sharing of sensitive information, some state and federal laws require a heightened standard of notice to or consent from users.[3]

Q 1.4 What is "non-personal information"?

Non-personal information can be defined as information about an individual that does not identify that individual in any way. Traditionally, the collection or disclosure of non-personal information has not been regulated by law. The concept of non-personal information, like the definition of PII, is evolving—but generally includes such things as demographic data, Internet browser information (for example, browser settings and browsing history, including dates and times of website visits), and "persistent identifiers" associated with Internet usage (for example, unique device identifiers, cookies, and

Internet Protocol (IP) addresses—the numbers assigned to desktop computers or other devices by which the Internet is accessed).

The dividing line between PII and non-personal information continues to be a topic of some debate. In some limited circumstances, information such as geolocation data and persistent identifiers, even without linkage to traditional types of PII such as name and email address, has been construed as PII, notably when the person whose information is being collected is a child.[4]

Q 1.5 What is a "persistent identifier"?

A persistent identifier is, as its name suggests, an identifier connected to a user that remains in place over time. For example, cookies (small text files kept on a user's Internet-enabled device that allow a web server to store information on the user's machine) are persistent identifiers that can be used to recognize a user's device (N.B.: not the user himself or herself) across different websites. In the mobile space, there are a few different types of persistent identifiers, including:

- a unique device identifier (UDID), which is a hardware ID that is permanently associated with the mobile device. Unlike cookies, which can be cleared to erase a specific user's actions, a UDID cannot be deleted;[5]
- a media access control (MAC) address, which is a unique identifier for identifying a piece of hardware (such as a mobile device) on a network. This "hardware address" for a mobile device therefore enables advertisers to track an individual phone as it moves across network connections;
- international mobile equipment identity (IMEI), which is essentially an electronic serial number, used in some countries to blacklist—in other words, to prevent from working on a mobile network—devices that have been identified as stolen;
- identifiers provided by app platforms, such as Apple's Identifier for Advertisers (IFA) and Apple Identifier for Vendors (IFV). The IFA and IFV behave more like online cookies and can be reset to avoid permanently linking any data with a specific user. Further, the IFA provides an opt-out mechanism to allow users to avoid behavioral targeting, and the IFV is deleted when a user deletes all apps from a specific developer.[6]

General Principles for Privacy Policies and Practices

Q 1.6 When should a company design its information privacy policies and practices?

There is no legal mandate that privacy issues be considered at any particular point in the development cycle of a product or service. But the FTC and others have strongly encouraged "privacy by design," which is the principle of considering information privacy issues from the very beginning, and then at every stage of growth and entry into new markets. It is easier to create and modify information privacy policies and practices when a company has kept information privacy in mind from the outset.

Privacy by design is discussed in further detail at Q 1.13, below.

Q 1.7 What are the general principles that a company must keep in mind when designing its information privacy policies and practices?

Here again, there is no explicit legal mandate, but regulators have encouraged attention to certain core principles. In a 1998 report,[7] the FTC identified the following five (now widely accepted) "Fair Information Practice Principles":

- **Notice/Awareness:** Users should be given notice of a company's information privacy policies and practices, particularly those involving the collection and use of PII.
- **Choice/Consent:** Users should have the ability to control whether and how their PII is being collected and used. Companies should provide users a way to give their consent for having their PII collected and used. Users should also have a choice regarding how their personal information actually will be used, especially for proposed uses extending beyond the use for which the information was collected.
- **Access/Participation:** Users should be able to access their own information, review it, and request changes to anything that is inaccurate or incomplete.

- **Integrity/Security:** Companies should implement reasonable security practices to protect consumer information, especially PII. (A detailed discussion of data security is outside the scope of this book, but there is some additional discussion of data security at Q 1.11.)
- **Enforcement/Redress:** Companies should put in place self-regulatory enforcement and redress mechanisms to ensure that they are following fair information privacy practices. Such mechanisms could include, for example, external audits and certifications.

Subsequent reports have identified an additional core principle that may be added to this list:

- **Focused collection/data minimization:** Companies should collect and retain only as much PII as needed to accomplish the purposes for which users disclosed the PII. Collected PII should be deleted as soon as it is no longer needed.

The principles listed above have served as the framework for many privacy laws and regulations and, thus, are important to keep in mind when designing a company's information privacy policies and practices.[8]

Notice

Q 1.8 How should a company provide notice to users of its information privacy practices?

Companies typically provide notice of their information privacy practices through a privacy policy made available to users on company websites and mobile applications. The content in a company's privacy policy will vary depending upon the industry involved and the applicable laws and regulations. Privacy policies generally should include information on the entity collecting the data, how the data will be used, any potential recipients of the data, the nature of the data collected, the means by which the data will be collected (if not obvious), whether the data collection is voluntary or mandatory, and the steps taken to ensure the confidentiality, integrity, and quality of the data collected.[9]

California law requires that a privacy policy be posted conspicuously and that it describe:

- the categories of PII being collected;
- the categories of third-party persons or entities with whom the information may be shared;
- any process for consumers to review and request changes to PII;
- the process for notifying consumers of changes to the operator's privacy policy;
- the effective date of the policy;
- how the operator responds to web browser "do not track" signals; and
- whether, based on usage of the site, other parties may collect PII about the user over time and across different websites.[10]

For further guidance on drafting a privacy policy, see chapter 2.

The California Consumer Privacy Act, which will go into effect January 1, 2020, requires that companies disclose, prior to or at the time of collection, what types of personal data are collected. At the time of this edition's publication, neither the courts nor the California Attorney General's office has weighed in on whether including disclosures in a website's privacy policy, which are already required under other California statutes as listed above, will be sufficient to meet this provision.

Consumer Choice and Consent

Q 1.9 What does "consumer choice and consent" mean?

Choice means providing customers with options regarding how and/or whether their personal information may be used. Choice/consent typically comes in one of two forms: (1) an opt-in, which means the customer takes an affirmative step to allow a company to collect

and/or use its information; and (2) an opt-out, which means the customer takes an affirmative step to prevent a company from collecting and/or using its information. When no affirmative steps are taken by the consumer, the company's default practice applies.[11]

Companies also should give users a way to withdraw or limit their consent to those uses that are consistent with the context in which the PII was originally disclosed.[12] The classic method of online consent is allowing the consumer to check an "I agree" box after being presented with the opportunity to review the privacy policy and terms of service.

Q 1.9.1 When must a company provide users with a choice concerning the use of their PII?

Consumer choice concerning the use of personal information is not necessary in all circumstances. The FTC has provided general guidance on when consumer consent should be obtained. According to the FTC, companies do not need to provide choice before collecting and using consumer information for practices that are consistent with the transaction or the company's relationship with the consumer (for example, after a consumer purchases an automobile, the dealer uses the consumer's address to send recall information or a coupon for an oil change), or are required or specifically authorized by law. Companies generally should provide consumers a choice "before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes."[13]

In addition, specific privacy statutes dictate that choices be available to users in certain circumstances. For example, the Gramm-Leach-Bliley Act (GLBA), which applies to financial institutions, requires covered businesses to provide consumers with the ability to opt out of having certain personal information shared with third parties (outside of specific enumerated exceptions).[14] Likewise, the California Consumer Privacy Act requires that businesses honor certain consumer requests to not have their data sold, or to have their personal data deleted.

Q 1.9.2 When is consumer consent to a company's information practices required?

Because a company's privacy policy serves as notice of its information practices, it is generally understood that users have consented to the practices described in the privacy policy when they use a company's services and submit their personal information. It is a best practice, and in some cases a legal requirement, to obtain the affirmative consent of users before collecting their information for certain purposes—particularly if the collection or the nature of how the data is used is sensitive or unexpected.

For more on affirmative consent, see chapter 2.

Access and Review

Q 1.10 What access to their PII must a company provide to consumers?

Access boils down to allowing consumers to view the personal information that a company has collected about them and to contest the data's accuracy or completeness. Regulators generally would say that companies are well advised to provide users with reasonable, timely, and inexpensive access to PII, as well as an easy mechanism to contest, delete, and update inaccurate or incomplete information.[15] When the California Consumer Privacy Act goes into effect in 2020, businesses will be required to disclose what categories of personal information they store for California consumers.

Data Security

Q 1.11 What should a company do to keep customer data secure?

There is no explicit and comprehensive legal standard for data security in the United States. Like data privacy, there is a patchwork of requirements including the FTC Act and state equivalents, some sector-specific laws for healthcare data and financial services data, common law, and other sources. The emerging view of enforcement

agencies like the FTC is that a company must have "reasonable" security, meaning that security practices must be continually modernized to be reasonable in light of emerging threats and best practices for defense. The obligation is not only to keep outside intruders from obtaining data, but also to keep data secure from negligent or malicious insiders, and to oversee vendors' security. In various contexts, companies have been required to use, or have been faulted for not using, such specific measures as encryption, robust access controls and password policies, multi-factor authentication, and a written incident response plan.

A detailed discussion of data security is outside the scope of this book. Readers seeking more information on data security and what to do to prevent or respond to a security breach should consult other resources dedicated to this topic.[16]

Enforcement

Q 1.12 What types of actions constitute violations of information privacy laws?

Companies have been deemed to violate information privacy laws where the company, among other things:

- fails to comply with its own privacy policy;[17]
- uses or shares data in a manner inconsistent with or not disclosed in a company's privacy policy;[18]
- collects and/or uses personal information without posting a privacy policy;[19]
- makes false representations in a privacy policy;[20]
- fails to implement reasonable security practices to protect the personal information of customers;[21] or
- collects, uses, or discloses personal information from children without notice to parents and/or parental consent.[22]

Q 1.12.1 Which agencies take enforcement action against privacy violations?

Just as no single law governs the protection of personal information, no single agency enforces data privacy laws. These laws are enforced by a number of federal and state regulatory authorities. The FTC and state attorneys general have become particularly active in this area, as have the U.S. Department of Health and Human Services (as to healthcare data) and various state and federal financial services agencies. Different laws designate different regulatory authorities for enforcement.

Individuals also have sought to enforce their rights through class action and individual lawsuits. For more information on the enforcement of privacy laws and related litigation, see chapter 9.

Privacy by Design[23]

Q 1.13 What is privacy by design?

Privacy by design is the approach of protecting individuals' privacy by integrating consideration of privacy issues from the very beginning of the development of products and services, business practices, and physical infrastructures. It can be contrasted to an alternative process where, for example, the privacy implications of a proposed product or service are not considered until just before launch. At that point, the relevant hardware or software may be close to "fully baked" and thus difficult to change to address any privacy issues. Privacy by design encourages consideration of privacy issues by all members of the development team, at an earlier and more conceptual stage.

Q 1.13.1 What are the basic principles of privacy by design?

The concept of "privacy by design" dates back at least to 1995, when it was advocated by the Information and Privacy Commissioner of Ontario, Canada; the Dutch Data Protection Authority; and the Netherlands Organisation for Applied Scientific Research. It is based on the following foundational principles:[24]

- **Prioritizing customer privacy:** The privacy interests of customers are paramount.
- **Proactive efforts:** Companies should take proactive efforts to anticipate privacy issues and implement measures to protect customer privacy.
- **Systematic implementation:** Companies should plan for and implement privacy protections systematically throughout every stage of research, design, and development of products and services.
- **Privacy embedded into design:** Privacy protections should be embedded into the design of all business practices, operations, and IT systems.

Q 1.13.2 How should a company implement privacy by design?

A company first should define its information privacy policies. These policies will provide the foundation on which operations and development teams can determine privacy requirements and design privacy safeguards. It is also recommended that a company designate an individual or group responsible for overseeing and enforcing privacy efforts from the beginning stages of every product and service development. It is then important that the privacy team be included in a meaningful way in design choices and reviews. A company also should conduct periodic reviews of privacy controls in new products, services, and programs. To the extent that a company is incorporating third-party content into its own products or services—such as when Company A plugs a software module from Company B into the code for Company A's mobile app—the company should review that third-party content, too, for its privacy implications.

PRACTICE TIP

Pragmatically speaking, for privacy professionals, "privacy by design" can be stated as: "Be sure the business invites you to the first meeting." The further a product or service is in the development process, the more likely it is that privacy choices have been made that would be difficult or costly to reverse or amend.

Legislative and Regulatory Framework

Federal Regulation

Q 1.14 What laws does the United States have concerning information privacy?

There is no single comprehensive U.S. law concerning the protection of all types of personal information. Instead, personal information is protected by an assortment of laws and regulations enacted at both the federal and state level. These include open-ended laws of general applicability that are now being applied to privacy issues, as well as laws that apply to specific industries (notably healthcare and financial services), or types of people (children), information, and activities.

Q 1.14.1 What are "general applicability" laws?

General applicability laws are laws that do not expressly mention privacy, but that nonetheless have been applied to privacy practices. The most important of these laws is the Federal Trade Commission Act (FTC Act), a consumer protection law that prohibits "unfair or deceptive acts or practices in or affecting commerce."[25] The FTC Act has been used frequently by the FTC to bring privacy enforcement actions against entities whose information practices have been deemed "unfair" or "deceptive."

Most states also have unfair and deceptive acts and practices (UDAP) statutes that substantially mirror the FTC Act and that have been applied in the privacy context. The state laws are often referred to as mini-FTC Acts. State regulation is discussed further at Q 1.18, below.

Q 1.15 What is the FTC?

The Federal Trade Commission is an independent agency of the U.S. government, governed by a chairman and four other commissioners, all nominated by the president and confirmed by the Senate.[26] The FTC's mission is to "prevent business practices that are anticompetitive or deceptive or unfair to consumers; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish this without unduly burdening legitimate business activity."[27]

Q 1.15.1 What authority does the FTC have to regulate privacy or bring privacy enforcement cases?

The FTC has authority to issue privacy *regulations* in circumstances defined by Congress; for example, the Children's Online Privacy Protection Act included a specific directive to the FTC to enact implementing regulations, which the FTC has done twice.[28] The FTC also has general authority to *enforce* consumer protection laws that prevent fraud, deception, and unfair business practices.[29] Enforcement (that is, to make specific cases against companies deemed to be in violation) occurs principally under section 5 of the FTC Act (15 U.S.C. § 45), which states that "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." The FTC has interpreted its authority to sanction "unfair and deceptive acts or practices" as encompassing the making of enforcement cases regarding how personal information is treated by companies.[30] Along with this general authority, the FTC is given by other laws specific statutory responsibility for issues such as children's privacy online and commercial email marketing.[31]

Q 1.16 What are "unfair" acts or practices?

An "unfair" act or practice under the FTC Act is defined as one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[32]

Broadly speaking, the FTC generally finds a practice "unfair" when the practice is intrinsically wrongful and causes substantial harm to consumers with no offsetting benefit. Substantial harm is typically monetary harm, such as a seller coercing a consumer into purchasing unwanted goods or services; emotional or other subjective harms are typically not considered substantial harm.[33] For example, failing to adequately protect customer data—particularly, but not only, if that data is later exposed through a breach—can be considered an "unfair" act or practice.[34]

Q 1.17 What are "deceptive" acts or practices?

A "deceptive" practice is one involving a "misrepresentation, omission, or other practice, that misleads the consumer acting reasonably in the circumstances, to the consumer's detriment."[35]

In the privacy context, the FTC generally finds practices deceptive when a company insufficiently discloses its privacy practices or engages in practices that are contrary to its disclosures. Specifically, if a company's use of consumer data does not match its privacy policy, it will be found to be deceptive. For example, the FTC has alleged deceptive practices where a company promised in its privacy policy that it would not share users' personally identifiable information with third parties, or would only use the PII in a way that was consistent with the purpose for which it was submitted, but then provided the information to advertisers.[36]

State Regulation

Q 1.18 What state laws apply to information privacy issues?

Most states have their own unfair and deceptive acts and practices statutes, or "UDAP" statutes. These statutes vary in substance and

strength from state to state—many have broad prohibitions against unfair *and* deceptive acts and practices,[37] while New York's, for example, is limited to deceptive acts.[38] Some states exempt certain industries, such as insurance[39] or utility companies,[40] from their UDAP laws. These statutes generally allow for private rights of action (*see* Q 2.19 *et seq.*).

The California Online Privacy Protection Act (CalOPPA) and the California Consumer Privacy Act provide specific privacy protections that are required for entities doing business in California.[41] For more on CalOPPA, see chapter 8.

Some states also have consumer financial privacy laws. GLBA expressly provides that it does not preempt state privacy laws that are not inconsistent with its provisions.[42] Many states, including California,[43] Texas,[44] and New York,[45] have enacted financial privacy laws that provide greater protection for consumers than GLBA and that are not preempted by GLBA.

Biometric privacy issues are attracting increased state attention. For example, the Illinois Biometric Information Privacy Act (IBIPA)[46] regulates the use of data from a person's retina or eye scan, fingerprint, hand scan, or facial geometry.[47] IBIPA requires companies to treat biometric information with a level of care that is the same as or greater than the care with which it treats PII or other sensitive information, such as account numbers, driver's license numbers, and Social Security numbers. Numerous class actions have been brought under the IBIPA on behalf of affected individuals.

State common law also can apply to information privacy. Tort theories such as intrusion upon seclusion, appropriation of name or likeness, right of publicity, and false light, as well as others, have all been invoked in privacy matters.[48]

Industry-Specific Regulation

Q 1.19 What types of industry-specific laws apply to information privacy issues?

The three most notable are the GLBA,[49] which applies to financial institutions, the Health Insurance Portability and Accountability Act of

1996 (HIPAA),[50] which applies to the healthcare industry, and COPPA,[51] which imposes extensive obligations on operators of websites or online services that collect and use personal information from children under thirteen years of age.

For more on privacy in industry-specific contexts, see chapters 3, 4, and 5.

Technology-Specific Regulation

Q 1.20 Are there any information privacy laws that apply specifically to audiovisual products?

Yes. The Video Privacy Protection Act (VPPA),[52] passed in 1988, was intended to prevent disclosure of information about consumers' video viewing habits. On its face, the statute applies to information about viewing of videocassettes and "similar audiovisual materials." Courts thus far have applied VPPA to newer forms of physical audiovisual products, such as videos, video games, DVDs, and Blu-ray discs. Courts thus far have also treated VPPA as applicable to viewing of streaming video on the Internet.

For more on the Video Privacy Protection Act, see chapter 8.

Q 1.21 Are there any information privacy laws or guidelines that apply specifically to mobile devices and applications?

Industry-specific privacy laws, such as GLBA and HIPAA, apply to mobile devices and applications designed for those industry purposes. If an application collects information about children, then COPPA applies. CalOPPA also applies to mobile devices. The Telephone Consumer Protection Act of 1991 (TCPA), which was originally enacted to prevent automated telemarketing, also has been applied to mobile devices.[53] The FTC and California attorney general have also issued general guidance on mobile privacy.

For more on mobile privacy laws and guidelines, see chapter 6.

PRACTICE TIP

Privacy considerations extend to marketing via text messages. For example, a class action suit in the Southern District of California alleges that unwanted text messages from Guess, Inc. violated TCPA. In March 2015, the district judge denied a motion to dismiss, holding that the plaintiff alleged facts sufficient to infer that Guess used an auto-dialer, which if used for unsolicited calls or texts, violates the statute.[54] Numerous similar TCPA class actions have been filed against other companies.[55]

For more on the Telephone Consumer Protection Act, see chapters 6 and 9.

Non-U.S. Regulation

Q 1.22 Do other countries have laws about information privacy with which U.S.-based companies must comply?

If a company has assets or employees abroad, operates in another country, or has a website or mobile application directed to or accessed by non-U.S. users, it needs to be aware of the potentially applicable laws in such other jurisdictions. This includes, for example, the European Union Data Protection Directive, which requires certain safeguards and disclosures before any personal data is processed; the EU ePrivacy Directive (EU cookie law), which requires websites to provide users with clear and comprehensive information when engaging in the storage of user information; and the EU General Data Protection Regulation (GDPR), which took effect in May 2018. The GDPR has also spurred other countries to enact further global privacy legislation, such as Brazil's Data Protection Law, known as Lei Geral de Protecao de Dados (LGPD).

The EU requirements are more restrictive than U.S. laws in a number of important respects. For instance, the EU Data Protection Directive *requires* companies doing business in the European Union to obtain

explicit opt-in consent from users prior to collecting and processing sensitive personal information.[56] It also requires companies to ensure that the third parties that may be processing consumer data have implemented certain information practices, specifically with regard to the security of the data.[57] The EU ePrivacy Directive[58] requires prior informed consent for storage of or access to information stored on a user's terminal equipment, unless the cookie is used for the sole purpose of carrying out the transmission of a communication or is necessary for a service provider to provide a service requested by a user.[59]

The GDPR replaced the Data Protection Directive as of May 25, 2018. The United States also has adopted a Privacy Shield, a mechanism for east-to-west data transfers across the Atlantic from Europe to the United States that is designed to permit such transfers in a manner that is compliant with the GDPR. The Privacy Shield replaced an earlier regime for such transfers, the Safe Harbor, which was invalidated in 2015 by the European Court of Justice.[60] More information about the GDPR and the Privacy Shield can be found in chapter 10.

In-depth coverage of non-U.S. privacy law is beyond the scope of this book. Readers seeking more information on approaches to privacy regulation in jurisdictions beyond the United States should consult other resources dedicated to international privacy laws.[61]

Guidance and Best Practices

Privacy Certifications

Q 1.23 What are privacy certifications, and are they necessary?

Nonprofit privacy seal programs—like TRUSTe[62]—allow a company to display their trustmark or seal, provided that the company adheres to their privacy requirements (and pays a fee). Such certifications are entirely optional. In order to grant their certification, such programs will typically conduct an upfront review or audit of a company's website and privacy statement to ensure compliance with their standards, recommend changes, and validate that any deficiencies are remediated. These certifications generally expire and must be renewed. While not necessary, displaying a privacy seal is one way in which

companies can try to signal to users that they disclose their information privacy practices and policies and that their privacy practices comply with fair information practice principles (*see* Q 1.7) and other privacy guidelines.[63]

PRACTICE TIP

Companies should vet a privacy certification program before relying on it. In March 2015, the FTC approved a final order against TRUSTe for failing to conduct annual re-certifications of participating companies and for misrepresenting its status as a nonprofit entity.[64]

Industry Guidelines and Codes of Conduct

Q 1.24 In addition to federal and state law, what guidance on information privacy should companies review and consider?

Companies can refer to industry guidelines and codes of conduct for additional guidance on information privacy. The FTC and other government offices also regularly issue guidance on privacy that, strictly speaking, does not have the force of law, but is still important for companies to consider. Examples include the following FTC reports, all available at ftc.gov:

- The annual *Privacy and Data Security Update* (at press time the most recent edition was January 18, 2018)
- *Internet of Things: Privacy & Security in a Connected World* (January 2015)
- *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012)[65]
- *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000)[66]

Companies should also review the nonbinding "Consumer Privacy Bill of Rights" issued by the White House in February 2012.[67] Each of these resources is discussed below in more detail at QQ 1.24.1–1.24.2.

Companies should also consider if guidelines exist for their specific products, services, or industries. For example, in January 2015, the FTC released *Internet of Things: Privacy and Security in a Connected World*,[68] a report geared towards the increasing number of businesses that create Internet-connected devices. The report outlines privacy and data security best practices for these businesses, such as security by design, oversight of third-party service provider security, and device access control measures. Additionally, the FTC and the National Telecommunications & Information Administration of the U.S. Department of Commerce have released various recommended industry practices, including the inclusion of "do-not-track" options on web browsers and mobile apps[69] (which are intended to disable the use of cookies that track users' browsing behavior) and measures that would provide for users to "opt in" rather than "opt out" of data collection and sharing.[70]

Additionally, some industry groups have adopted privacy codes of conduct or other forms of self-regulatory regimes. Certain regimes make compliance with the code of conduct a prerequisite for membership in an industry association, as well as requiring external audits and certifications to verify such compliance.[71] For example, the Digital Advertising Alliance and the Interactive Advertising Bureau include a number of self-regulatory principles related to digital advertising that member organizations must pledge to follow.[72] A company should check with any industry associations of which it is a member to see if it is required to adhere to any specific codes of conduct.

Q 1.24.1 What best practices are included in the FTC report *Protecting Consumer Privacy in an Era of Rapid Change?*

In this 2012 FTC Report, the FTC outlines its final privacy framework and implementation recommendations, which were "intended to articulate best practices for companies that collect and use consumer [personal] data."[73] Companies that collect only non-sensitive information from fewer than 5,000 users per year and do not share

that information with third parties are not expected to adhere to the privacy framework. Expanding upon the fair information practice principles issued by the FTC in 1998 (*see* Q 1.7), the framework presents three basic principles:

- **Privacy by design:** "Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services";
- **Simplified consumer choice:** "Companies [should] simplify consumer choice by presenting important choices—in a streamlined way—to consumers at the time they are making decisions about their data"; and
- **Transparency:** "Companies should increase the transparency of their data practices."[74]

In addition to these overarching principles, the FTC also identified the following areas of focus:

- **Do not track:** Mechanism for users to identify if they do not wish to be tracked for purposes of online behavioral advertising;
- **Mobile:** Provide improved privacy protections, specifically development of "short, meaningful disclosures" for mobile services;
- **Data brokers:** Passage of laws providing customers with access to personal information about them held by data brokers that are not already covered by the Fair Credit Reporting Act (FRCA) (for more information on the FRCA, see chapter 4);
- **Large platform providers:** Examination of large platforms, such as Internet service providers, operating systems, browsers and social media, and their practices of comprehensively tracking users' online activities ("comprehensive tracking"); and
- **Providing enforceable self-regulatory codes:** Facilitation of the development of sector-specific codes of conduct.[75]

Social Media

Q 1.25 What privacy concerns are raised for a company that integrates social media into its business plans?

Most companies now integrate social media into their business plans as an important way of interacting with customers and attracting new business. Companies should be aware of the extent to which, by integrating with social media tools that have their own privacy practices, they may be opening their consumers to uses of their data that are not specifically contemplated in the companies' own privacy policies. Disclosure of social media integration is generally advisable.

PRIVACY FACT

"Social media" refers to websites, applications, and other online tools that allow users to create or share information by interacting with other people or organizations. Social media can take many different forms, including but not limited to blogs, wikis, online social networks, Twitter, Facebook, YouTube, LinkedIn, FourSquare, Pinterest, Wikipedia, Yammer, websites, podcasts, virtual worlds, listservs, photo-sharing sites (like Instagram), and other forms of online publishing and sharing. Social media can be used for either business or personal purposes.

Future Outlook

Q 1.26 What does the future hold for information privacy laws?

Information privacy law is a highly dynamic area. Additional legislation, regulation, enforcement actions, and court decisions can be expected. New privacy legislation is introduced in Congress and state legislatures on a regular basis, and the state and federal courts deal

with a never-ending stream of potentially precedent-setting privacy cases. As this book went to press, for example, California had just passed the California Consumer Privacy Act which, when it goes into effect in 2020, will provide California consumers with a wide range of rights regarding the collection, use, and sale of their data. These rights have significant corresponding obligations for most businesses, and the act is likely to reshape U.S. privacy law much as the GDPR has reshaped European privacy law. In the judiciary, the U.S. Supreme Court held in 2018 that "the Government will generally need a warrant" to obtain cell-site location information—the records kept by wireless carriers of the physical locations of their customers' cell phones.[76] The holding that customers have a protectable expectation of privacy in cell-site location information may have significant implications for privacy law generally, going beyond the criminal law context in which the Supreme Court issued its ruling. Attention to new legal developments, both legislative and judicial, therefore, is an important element of any company's privacy compliance program.[77]

Notes to Chapter 1

1. For more specific and detailed definitions of what constitutes personal information under particular federal statutes, see chapters 3, 4, and 5. The definition of personal information may also vary by state. *See, e.g.*, CAL. CIV. CODE § 1798.80(e); 201 MASS. CODE REGS. 17.02 (defining personal information as a Massachusetts resident's first name or initial plus last name, together with one or more of (a) Social Security number, (b) driver's license number, or (c) financial account number or credit or debit card number; excluding information lawfully obtained from public sources or government records).

2. *See, e.g.*, CAL. CIV. CODE § 1798.80(e); SEC Regulation S-P, 17 C.F.R. pt. 248 (implementing Gramm-Leach-Bliley Act's privacy provisions for financial institutions; definition of nonpublic personal information "consists, generally speaking, of [ ] personally identifiable financial information . . . [and] excludes publicly available information"), www.sec.gov/rules/final/34-42974.htm.

3. For more information regarding the disclosure of certain types of sensitive information, see chapter 4 (discussing disclosures of financial institutions), chapter 5 (discussing protected health information), and chapter 3 (discussing the personal information of children under thirteen).

4. 16 C.F.R. § 312.2 (definition of "personal information" at (7) and (9)); *see* Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy & Identity Protection, Federal Trade Comm'n (May 15, 2013), www.ftc.gov/sites/default/files/attachments/press-releases/ftc-sends-educational-letters-businesses-help-them-prepare-coppa-update/130515coppadomesticidentifiersletter.pdf; *see also infra* chapter 3.

5. Christopher G. Cwalina, Richard Raysman & Steven B. Roosa, *Mobile App Privacy: The Hidden Risks*, Practice Note, at 5 (Practical Law Co. 2013).

6. *Apple's IFA vs. IFV: When to Use Which and Why*, TUNE HELP (Aug. 10, 2015), http://support.mobileapptracking.com/entries/22207575-Apple-s-IFA-vs-IFV-When-To-Use-Which-and-Why.

7. FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS (June 1998) [hereinafter 1998 FTC REPORT], www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/priv-23a.pdf.

8. *See also* The Consumer Privacy Bill of Rights, attached as Appendix A to THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (Feb. 2012) [hereinafter The Consumer Privacy Bill of Rights], www.whitehouse.gov/sites/default/files/privacy-final.pdf; Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015 (Feb. 2015) [hereinafter CPBRA], www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf; FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID

CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (Mar. 2012) [hereinafter 2012 FTC REPORT], www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

9. *See* 1998 FTC Report, *supra* note 7, at 7–8.

10. CAL. BUS. & PROF. CODE § 22575.

11. 1998 FTC Report, *supra* note 7, at 8–9.

12. *See* The Consumer Privacy Bill of Rights, *supra* note 8, at 47; *see also* CPBRA, *supra* note 8, at 7.

13. *See* 2012 FTC REPORT, *supra* note 8, at vii–viii.

14. *See* 15 U.S.C. § 6802.

15. *See* 1998 FTC REPORT, *supra* note 7, at 9.

16. *See, e.g.*, updates on data security regularly posted by the authors to www.debevoisedata.com; MCNICHOLS & MOHAN, CYBERSECURITY: A PRACTICAL GUIDE TO THE LAW OF CYBER RISK (PLI 2015); MATHEWS, PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE (2d ed. PLI 2016).

17. *See, e.g.*, Consent Decree and Order for Civil Penalties, Permanent Injunction and Other Relief, United States v. Path, 13-cv-0448 (N.D. Cal. Feb. 8, 2013).

18. *See, e.g.*, Press Release, Fed. Trade Comm'n, Gateway Learning Settles FTC Privacy Charges: Company Rented Customer Information It Pledged to Keep Private (July 7, 2004), www.ftc.gov/news-events/press-releases/2004/07/gateway-learning-settles-ftc-privacy-charges.

19. *See* CAL. BUS. & PROF. CODE § 22575(a).

20. *See, e.g.*, Press Release, Fed. Trade Comm'n, Microsoft Settles FTC Charges Alleging False Security and Privacy Policies (Aug. 8, 2002), www.ftc.gov/news-events/press-releases/2002/08/microsoft-settles-ftc-charges-alleging-false-security-privacy.

21. *See, e.g.*, Press Release, Fed. Trade Comm'n, BJ's Wholesale Club Settles FTC Charges (June 16, 2005), www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges.

22. For more information on children's privacy, see chapter 3.

23. For more information on privacy by design, see 2012 FTC REPORT, *supra* note 8, at 22–34; *see also* ANN CAVOUKIAN, OPERATIONALIZING PRIVACY BY DESIGN: A GUIDE TO IMPLEMENTING STRONG PRIVACY PRACTICES (Dec. 2012) (a paper by former Information and Privacy Commissioner of Ontario, a privacy expert, and creator of the concept of privacy by design), www.ipc.on.ca/images/Resources/operationalizing-pbd-guide.pdf.

24. *See* 2012 FTC REPORT, *supra* note 8, at vii–viii; CAVOUKIAN, *supra* note 23, at 12.

25. 15 U.S.C. § 45(a).

26. *See Commissioners*, FED. TRADE COMM'N, www.ftc.gov/about-ftc/commissioners (last visited June 6, 2016).

27. *See About the FTC*, FED. TRADE COMM'N, www.ftc.gov/about-ftc (last visited June 6, 2016).

28. *See* 15 U.S.C. §§ 6501–06.

29. *See id.* § 45(a).

30. *See, e.g.*, Consent Decree and Order for Civil Penalties, Permanent Injunction and Other Relief, United States v. Path, 13-cv-0448 (N.D. Cal. Feb. 8, 2013) (alleging that defendant, Path, violated the FTC Act and COPPA by making deceptive representations regarding the automatic collection of information from consumers' mobile device address books); Press Release, Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented (Google settled for $22.5 million with the FTC over allegations that it misrepresented privacy assurances to users of Safari). The Third Circuit recently held that the FTC has the authority to bring lawsuits against corporations regarding reasonable data security standards. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 247 (3d Cir. 2015).

31. *See* Children's Online Privacy Protection Act, 15 U.S.C. § 6501–06; Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), 15 U.S.C. §§ 7701–13.

32. 15 U.S.C. § 45(n).

33. *See FTC Policy Statement on Unfairness*, FED. TRADE COMM'N (Dec. 17, 1980), www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

34. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 247 (3d Cir. 2015); Press Release, Fed. Trade Comm'n, FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy (Aug. 29, 2013), www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers.

35. *FTC Policy Statement on Deception*, FED. TRADE COMM'N (Oct. 14, 1983), www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

36. *See* Press Release, Fed. Trade Comm'n, Myspace Settles FTC Charges That It Misled Millions of Users About Sharing Personal Information with Advertisers (May 8, 2012), www.ftc.gov/news-events/press-releases/2012/05/myspace-settles-ftc-charges-it-misled-millions-users-about; *see also* FTC Notice, Myspace, LLC; Analysis of Proposed Consent Order to Aid Public Comment, 77 Fed. Reg. 28,388 (May 14, 2012).

37. *See, e.g.*, CAL. BUS. & PROF. CODE § 17200; CONN. GEN. STAT. § 42-110a; 815 ILL. COMP. STAT. 505; ME. REV. STAT. ANN. tit. 5 § 205A; MASS. GEN. LAWS ANN. ch. 93A, § 2.

38. N.Y. GEN. BUS. LAW § 349.

39. *See, e.g.*, FLA. STAT. ANN. § 501.212(4); LA. STAT. ANN. § 51:4106(1); MD. CODE ANN., COM. LAW § 13-104(1).

40. *See, e.g.*, LA. STAT. ANN. § 51:1406(1); MD. CODE ANN., COM. LAW § 13-104(2); MONT. CODE § 30-14-105; NEB. REV. STAT. § 59-1617(1); N.H. REV. STAT. § 358-A:3(I).

41. CAL. BUS. & PROF. CODE §§ 22575–79.

42. 15 U.S.C. § 6824.
43. 10 CAL. CODE REGS. § 2689.1 *et seq.*
44. 28 TEX. ADMIN. CODE § 22.4 *et seq.*
45. N.Y. COMP. CODES R. & REGS. tit. 11, §§ 420.0–420.24 (2001).
46. 740 ILL. COMP. STAT. 14/1 (2008).
47. IBIPA explicitly excludes many methods that could be used to identify a person, such as X-rays, MRIs, writing samples, photographs, and biological samples. 740 ILL. COMP. STAT. 14/10 (2008).
48. *See, e.g., In re* Google, Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 149–50 (3d Cir. 2015) (applying intrusion theory to alleged overriding of Internet browser privacy settings).
49. 15 U.S.C. §§ 6801–09.
50. 42 U.S.C. § 201 *et seq.*
51. 15 U.S.C. § 6501–06.
52. 18 U.S.C. § 2710.
53. 47 U.S.C. § 227; *see also* Satterfield v. Simon & Schuster, Inc., 569 F.3d 946 (9th Cir. 2009) (TCPA class action arising from text message sent to consumers' cell phones advertising publication of novel).
54. Haghayeghi v. Guess?, Inc., 2015 WL 1345302, at *7 (S.D. Cal. Mar. 24, 2015).
55. *See, e.g.*, Complaint, Nelson v. PVH Corp., No. 8:15-cv-00512 (C.D. Cal. Apr. 2, 2015) (class action alleging that PVH, a clothing company that owns brands such as Calvin Klein and Tommy Hilfiger, violated the TCPA by sending thousands of unrequested text message to customers).
56. Commission Directive 95/46/EC, of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, art. 8(2)(a) [hereinafter EU Data Protection Directive].
57. *Id.* art. 17(2).
58. Council Directive 2002/58/EC, of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002 O.J. (L 201), 37–47 [hereinafter EU ePrivacy Directive], http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN.
59. *Id.* art. 5(3); *see also* European Commission Article 29 Data Protection Working Party, Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies, WP 208 (Oct. 2, 2013), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf.
60. Case No. C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. (Oct. 6, 2015), http://curia.europa.eu/juris/documents.jsf?num=C-362/14.
61. *See, e.g.*, MATHEWS, *supra* note 16.
62. *See* TRUSTE, www.truste.com (last visited June 6, 2016).
63. For example, TRUSTe's certification standards are based on the fair information practice principles (*see* Q 1.7), OECD privacy guidelines, the APEC

privacy framework, and the U.S.-EU & U.S.-Swiss safe harbor principles. *See Enterprise Privacy Certification Standards*, TRUSTe (Mar. 12, 2015), www.truste.com/privacy-certification-standards/program-requirements/.

64. *See* Decision and Order, *In re* True Ultimate Standards Everywhere, Inc., No. C-4512 (F.T.C. Mar. 12, 2015); *see also* Press Release, Fed. Trade Comm'n, FTC Approves Final Order in TRUSTe Privacy Case (Mar. 18, 2015), www.ftc.gov/news-events/press-releases/2015/03/ftc-approves-final-order-truste-privacy-case.

65. 2012 FTC REPORT, *supra* note 8.

66. FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (May 2000) [hereinafter 2000 FTC Report], www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf.

67. The Consumer Privacy Bill of Rights, *supra* note 8.

68. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (Jan. 2015), www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

69. *See* FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 6–7 (Feb. 2013), www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf; *see also* Press Release, Fed. Trade Comm'n, FTC Staff Report Recommends Ways to Improve Mobile Privacy Disclosures (Feb. 1, 2013), www.ftc.gov/news-events/press-releases/2013/02/ftc-staff-report-recommends-ways-improve-mobile-privacy.

70. *See, e.g.*, 2012 FTC REPORT, *supra* note 8, at 57 n.24.

71. *See* 1998 FTC REPORT, *supra* note 7, at 10.

72. *The DAA Self-Regulatory Principles*, DIG. ADVERT. ALL., www.aboutads.info/principles (last visited June 6, 2016); Am. Ass'n of Advert. Agencies et al., Self-Regulatory Principles for Online Behavioral Advertising (July 2009), www.ana.net/advocacy/getfile/15279.

73. 2012 FTC REPORT, *supra* note 8, at iii.

74. *Id.* at vii, viii, 2–3.

75. *Id.* at v–vi.

76. Carpenter v. United States, __ U.S. __, __ (June 22, 2018).

77. *See, e.g.*, Russell Brandom, "After Facebook hearing, senators roll out new bill restraining online data use," https://www.theverge.com/2018/4/10/17221046/facebook-data-consent-act-privacy-bill-markey-blumenthal (Apr. 10, 2018).