

Privacy and Data Security
is for EVERYONE

Kirk J. Nahra, CIPP/US, Wiley Rein

This is a commonly accepted statement, is largely true, and is completely misleading. There is virtually no company in the U.S. that does not have specific legal obligations and risks related to the privacy and security of personal data. The details may change, depending on the industry and a company's practices. But for most companies, there is a core set of common obligations in an exceedingly complicated area, where the compliance challenges and legal risks are only growing.

Early privacy law in the U.S. was very different than how we think about it today. For many years, privacy law was almost entirely a question of what the government could do vis-à-vis individuals, in areas such as search and seizure, abortion rights, birth control and disclosure of suspicious affiliations. There was a common law tort of invasion of privacy, but this tended to be a “personal injury” issue, typically pitting one individual against another. Obviously, today, with the Edward Snowden revelations and other questionable government activities, this issue of the government’s ability to monitor its citizens is back on the front burner (and front pages).

In the mid-1990s, “privacy” began to develop a new identity in the United States, as companies began to be measured and evaluated based on how they gathered and used personal data about individuals — whether employees, customers or others. The European Privacy Directive was adopted in 1995 and still dominates much of the privacy policy debate today. As the internet era began, Congress began to debate how to control the activities of companies on the internet (with little progress other than substantial handwringing and grandiose pontificating). Children were given certain privacy rights on the internet (Congress only was able to protect children under the age of 13). The Children’s Online Privacy Protection Act protecting young children was followed closely by the Gramm-Leach-Bliley Act for financial services companies and the Health Insurance Portability and Accountability Act for the health care industry, which became strong and effective (although limited) privacy controls and led in part to the overall perception of a “sector-” and “practice-specific” privacy approach.

Now, through the passage of hundreds of laws and regulations at the state, national and

international levels, this perception needs to be re-evaluated. We can continue to debate with the European Union whether U.S. privacy law should be “adequate” in the eyes of the EU. However, it is clear that the volume of privacy and data security laws is so extensive — and the reach so pervasive — that virtually every company in this country has material obligations related to privacy and data security, for personal data involving employees, customers and others.

It is clear that the volume of privacy and data security laws is so extensive — and the reach so pervasive — that virtually every company in this country has material obligations related to privacy and data security.

These obligations are detailed, often overlapping and complicated, and create ongoing risks for litigation, business disputes, and government enforcement. Every company — particularly those in industries that do not have specific industry privacy and security laws — needs to adjust to this new world order of privacy and data security and ensure that appropriate steps are taken to evaluate risk and manage potential legal exposure.

What do most companies have to worry about?

Treatises covering thousands of pages try to detail the full range of privacy and security laws in the U.S. Here, we will focus only on the key elements that affect most companies. Obviously,

banks, health care companies, tax preparers, or telecommunications companies (or service providers to these entities) have to worry about the comprehensive compliance regimes for those industries. For everyone else, here are the key components of the privacy and data security universe to understand.

Overall data security

The easiest piece to start with is the obligation of every company to protect the security of sensitive personal data, although, technically, this only applies to companies that have customers or employees.

Starting with the B.J.'s Wholesale case in 2005, the U.S. Federal Trade Commission has taken the position — supplemented by enforcement in more than 50 cases — that all companies have the obligation to implement reasonable and appropriate safeguards for the protection of personal data. Although the FTC's approach has been subject to expanded challenges, particularly in cases involving Wyndham Hotels (where the FTC won) and LabMD (with the FTC winning so far), the FTC has enforced this position regardless of specific statutory requirements for data security and any commitments made by companies to their employees or customers.

Although the FTC's requirements are not voluminous, they require ongoing activity from companies involving the security of personal data. To meet the FTC's requirements for a "reasonable and appropriate" data security program, the company must:

- Develop and implement a written comprehensive information security program that is appropriate to the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of the customer information at issue.
- Develop a security program that (1) ensures the security and confidentiality of customer information; (2) protects against "any" reasonably anticipated threats to security or integrity of information; and (3) protects against unauthorized access that could result

in substantial harm or inconvenience.

- Designate specific employees to coordinate security.
- Identify reasonably foreseeable risks and assess sufficiency of safeguards.
- Oversee service providers through due diligence and requiring contractual security standards.
- Evaluate and adjust program in light of changes.

These requirements have significant flexibility, but require a thoughtful, proactive security program that spans a company's full operations and keeps pace with ongoing changes in both business operations and technological evolution connected to information security.

HIPAA

Although the focus of HIPAA privacy and security rules is on the health care industry, these rules set out obligations that apply to a large volume of companies across many industries. This is not the place for a full evaluation of HIPAA's detailed requirements, but companies must consider HIPAA's requirements if any of these categories apply to them:

- They are in the health care business as a health care provider or health plan.
- They contract with companies in the health care business (i.e., a service provider to health care companies).
- They contract with companies who contract with companies in the health care business (and onward downstream indefinitely).
- They provide health care benefits to their employees (the broadest and least understood category of requirements).

In addition, there are many companies that must pay attention to and analyze HIPAA's requirements because they use or disclose health care information, even if they are not directly

regulated by the HIPAA rules. Accordingly, although HIPAA is not an overall privacy and security rule, it covers a large range of companies, many of whom may not be aware of their responsibilities.

Website privacy policy

For any companies that operate a website in the United States, it also has become common practice to develop an appropriate website privacy policy. The detail and challenge for these policies varies significantly based on what the website does and what information is collected. Although there are a limited number of laws defining specific responsibilities for these policies, at a minimum most companies must (1) ensure they do not run afoul of the FTC, by making sure the privacy policy is complete and accurate; and (2) meeting the specific requirements of California's law on website privacy practices, including the core components for such a policy and the recent changes involving do not track commitments.

Telemarketing/email marketing

Another key area of privacy regulation for most companies in the U.S. involves regulation of various marketing approaches. The "Do Not Call" laws (including the various federal components and the supplementing state laws) are among the most successful privacy laws (at least from the consumer perspective) because individuals seem to care about these issues and have in droves signed up for do-not-call registries. These issues only affect companies that conduct telemarketing. For them, this is a big deal.

On a broader level, the CAN-SPAM law that deals with email marketing has a broader application to a wide range of companies. This law applies to a wide variety of communications, not all of which are obviously "marketing." In addition, it applies to both personal and commercial communications, and requires a series of complicated (although relatively modest) steps for compliance. Aside from obvious marketers, such as retailers, this law is affecting the business practices of trade associations,

universities, professional services firms and many others. Canada has recently adopted its own version of CAN-SPAM, called CASL, which requires more aggressive front-end consent from individuals. If a company engages in any activity that could be construed as marketing through email, it must make sure to comply with these provisions.

Breach notification

The last "generally applicable" privacy and data security provision involves the laws in virtually every state addressing notification to individuals in the event of a security breach. Although these laws apply (in most situations) to only a limited range of personal information (such as Social Security numbers and credit card numbers), these are pieces of information that are held at least to some extent by virtually every company, at least as an employer. Now, states are adding other data elements (such as health care information in California) that expand the reach of these statutes. And, because these laws apply to protect individuals residing in a state, the laws apply to any kind of company, large or small, regardless of industry or geographic location.

These laws, at a minimum, require notification to individuals if their personal information is subject to a security breach (as defined by each law). Some laws require notification to state attorneys general as well. Although typically not required by laws, these notifications often (as is becoming a standard practice) incorporate credit monitoring services and other protections for individuals. There are certain relatively common terms to these laws, but there also are a wide variety of state-specific provisions that turn any breach involving individuals in multiple states into a significant compliance challenge. Because these notification letters typically become public, they also increase the likelihood of litigation or enforcement (as well as adverse publicity). Although the explicit goal of these laws is to provide notification to individuals, so that they can take action as appropriate (for example, to protect against identity theft), these laws also have had the effect of improving overall information security practices.

International implications

This article focuses on the array of U.S. laws and regulations that have broad impact. In addition, many companies will need to pay attention to the global privacy and data security environment. The EU has been the most active international privacy regulator, with the original EU rules going back to the 1990s.

The EU is in the midst of a dramatic revision to their privacy rules — the General Data Protection Regulation — which will require

compliance in 2018. Companies will be impacted by these rules across the globe. In the United States, the EU rules also present the companion challenge of creating difficulties in cross-border data transfers — mainly the transfer of data from the EU to the U.S. There are various options available to companies — including the new Privacy Shield program, standard contractual clauses, and binding corporate rules, but these challenges are extensive. Moreover, as more and more countries implement broad privacy laws, these challenges will only grow in volume and complexity.

Effective privacy and data security practices are an essential component of the operations of any business.

Privacy and data security issues are not going away. New laws and regulations are added to the books regularly. Enforcement, although still modest, is growing. Litigation also is growing. And ongoing developments involving the risks and benefits of big data make certain that the complexity of this environment will continue to grow. Effective privacy and data security practices are an essential component of the operations of any business. Although the challenges may seem daunting, the most important step for companies is to understand their general level of exposure, and to undertake a creative, thoughtful and thorough assessment of their privacy and data security activities, so they can manage these growing risks effectively.



DISTINGUISH YOURSELF

With CIP/US Certification.

iapp.org/certify/cipp/