Privacy Law for Security Professionals

By Kirk J. Nahra
ICIT Fellow and Partner, WilmerHale

Security existed as a business norm long before it became a legal and compliance requirement. Doctors' offices locked their doors at night to ensure no one could access their records. Stores took precautions when they walked the daily cash receipts to the bank. Now, it is enormously more complicated to guarantee data security, which is the physical and technological protection of both personal data and sensitive proprietary information. Appropriate best practices and legal requirements are growing every day, across all industries, and around the world.

At the same time, in a somewhat parallel development that has slightly preceded data security as a legal obligation, companies all over the world now need to make sure they are following appropriate practices relating to how personal information is collected, used, and disclosed. This growing range of privacy obligations should be understood generally by information security professionals, and an effective partnership with company privacy officials is critical to the appropriate protection of companies, their employees, their customers, and any other individuals whose data is being collected by these companies.

> *"Security existed as a business norm long before it became a legal and compliance requirement."*
>
> - Kirk Nahra

We should start with a few definitions. Privacy, data security, and cybersecurity are similar terms, yet have distinct definitions. While these terms are not defined in any specific law, the following definitions reflect common usage in the field. The term "*Privacy*" relates to the laws, regulations, and practices surrounding how personal data is used, gathered, maintained, and disclosed. "*Security*" (or "*Data Security*") refers to the laws, regulations, and practices surrounding how personal information is protected from unintended and unpermitted activity. More succinctly, it encapsulates the practices that protect data.

Of course, we have all heard the term "*Cybersecurity*," which relates to the protection of overall technological infrastructure. This term tends to be focused on national security and internet interconnections, which may or may not involve personal data. This means cybersecurity can be broader than data security, but also narrower in some ways because it does not include the security of paper records or physical information containers such as people. "Information

Security" encapsulates physical, cyber, and contextual processes and procedures governing the confidentiality, availability, integrity, and access of data and data containers.

Today, most privacy laws follow an approach established under a concept called *"Fair Information Practices*." This set of five principles dictates certain practices that should be included in privacy laws. The practices are:

1. Notice - Consumers should be notified of how companies will use and disclose their personal data.
2. Choice/Consent - Consumers have some right to choose how their data will be used.
3. Access - Consumers can see or copy their personal information.
4. Security - Sensitive data is appropriately protected from unpermitted or unauthorized uses and disclosures.
5. Enforcement – Controls must be implemented to ensure that the law is followed.

> "It will be critical for privacy and security professionals to work together to provide appropriate business strategies and effective protections for both companies and consumers."
>
> - Kirk Nahra

What are the Key Legal Principles in Modern Privacy Law?

The privacy framework in the United States is as follows.

- There are a large (and growing) number of laws and regulations at state, federal, and international levels.
- These laws have (to date) been specific by industry segment (e.g., health care, banking) or by practice (e.g., telemarketing).
- Today, there is no generally applicable US national privacy law covering all industries and all data.
- Because of the volume of laws and the fact that they are not "generally applicable," there is an increasing complexity of the regulatory environment.
- Many privacy laws have detailed obligations for contracts with vendors.
- There has been relatively limited enforcement, despite there being many agencies with enforcement authority; however, this enforcement seems to be growing.
- There also has been a relatively limited but growing range of litigation concerning privacy and security practices (focused primarily on data breach situations)
- There is an increasing concern, from privacy advocates, consumers, regulators, and others, about "big data," artificial intelligence, and otherwise unregulated personal data.

There also is an expanding international framework for privacy law. At the international level,

- There are separate privacy and security rules related to data in and coming from foreign countries.

- Where these laws exist, the rules usually are tougher in other countries – meaning that they are more protective of individual privacy (e.g., the General Data Protection Regulation in the European Union).
- An increasing number of countries do have privacy rules – and the rules are changing dramatically on an ongoing basis.
- Because of this complexity and ongoing change, there is significant disarray for companies operating on a global level to adjust to these changes in real-time.
- Many of these international laws apply to US companies, even if they have no physical presence in those countries.

There also are separate legal requirements related to data security. Security is now a separate legal requirement in the US – connected to privacy but with different rules and issues. Accordingly, data security has moved from a business-driven "best practice" to a legal requirement in all industries in the United States, and is developing as a global issue, but more slowly.

Which Laws are Most Important?

A critical challenge for most companies is identifying the laws that are relevant to their operations. These can be directly relevant, meaning that the law applies to a company in its own right, or can be applicable to companies through service-provider relationships, either by law or by contract. In thinking about most privacy laws, it is typically important to ask several key questions to assess how the law could potentially apply to a company or a consumer. These questions include:

- Who does the law apply to?
- Who does the law protect?
- What information is covered by the law? If you are covered by the law, what can and cannot be done with the personal information subject to the law?
- What rights apply to the information?
- What is the enforcement mechanism for the law?
- What does this law impact?
- Who does this law benefit or harm?
- What happens when the law does not apply or does not tell you what to do?

A small sampling of these laws is below, but any security professional should work with their company's privacy or legal teams to understand which laws are relevant to their company.

Industry Laws

US privacy law often is directed at specific industries. The *Health Insurance Portability and Accountability Act* (HIPAA) includes privacy and security rules which primarily apply to health care providers and public and private companies who store, process, or transfer health data. This law also applies to service providers to these entities, called "business associates."

The *Gramm-Leach-Bliley Act* (GLBA) protects the privacy and security of consumer information held by "financial institutions" such as banks, insurers, credit card companies, and other defined financial entities. The law requires these companies to give consumers privacy notices explaining their information-sharing practices. The law also gives consumers the right to "opt-out" of sharing information with some nonaffiliated third parties.

The *Family Educational Rights and Privacy Act* (FERPA) guards the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the US Department of Education, meaning virtually all colleges, universities, and public high schools. This law gives parents certain rights with respect to their children's education records, but primarily gives students the ability to control how their educational information is used and disclosed outside of the education environment.

Practice-Specific Laws

In addition to these “industry” laws, many US laws address particular practices. For example, the *Children's Online Privacy Protection Act* (COPPA) is designed to limit the collection and use of personal information about children under the age of 13 by the operators of internet services and websites.

The *Telephone Consumer Protection Act* (TCPA) is one of the many laws applicable to marketing activities, restricting telemarketing calls, the use of automatic telephone dialing systems, and artificial or prerecorded voice messages, even outside of the marketing context.

The *Controlling the Assault of Non-Solicited Pornography and Marketing* (CAN-SPAM) *Act* regulates the use of e-mail for marketing purposes.

“Overall” Privacy Laws

In recent years, we also have seen increased attention being paid to “overall” privacy laws; in other words, laws that impose regulations across industries and across practices. First, we have the *General Data Protection Regulation* ("GDPR") that protects the privacy of individuals in Europe, replacing a previous European Privacy Directive. The GDPR applies across industries, protecting all personal information. It has meaningful extra-territorial reach and applies to many US companies that do not have a physical presence in Europe.

The most recent development in this area involves the US. Currently, most attention is being paid to the *California Consumer Privacy Act* (CCPA). This law, which went into effect on January 1, 2020, protects the privacy rights of all California residents. While it does not apply in all contexts (e.g., non-profits are excluded from coverage, the law does not currently apply to employee data, and there are other exceptions), it is neither sector-specific nor practice-specific. Many states are evaluating whether to pass similar laws. This discussion has also led to a significant debate at the federal level about a national US privacy law.

Data Breach Notification Laws

One area with critical and direct overlap between privacy and security involves a broad range of laws that dictate a company's actions following a data breach. These laws began at the state level, starting with California, and now apply in all 50 states and the District of Columbia. There are a separate set of data breach notification rules as part of HIPAA, and new data breach reporting provisions in Europe as part of GDPR. In the US, these laws generally require notification of individuals when certain categories of personal information (e.g., Social Security Number, credit card number or bank account information, along with other data elements depending on the state) are the subject of a data breach, and there is some meaningful level of risk to the individual from the data breach. Many of these laws also require reporting to state government officials, such as a state attorney general.

Enforcement

The enforcement of US privacy law is dispersed across a wide number of government agencies. Many of the laws designate a specific enforcement agency. For example, the US Department of Health and Human Services' Office for Civil Rights is the primary enforcement agency for HIPAA. State attorneys general have broad enforcement authority over privacy and security, both through specific laws, like data breach notification laws, and through their general authority over consumer protection. The US Department of Justice often has criminal authority in, particularly egregious situations.

> "Privacy issues increasingly impact virtually all companies in all industries."
>
> - Kirk Nahra

In addition to specific agencies, the Federal Trade Commission (FTC) has a "catch-all" authority on privacy and security practices. The basic consumer-protection statute enforced by the FTC is Section 5(a) of the *FTC Act*, which prohibits unfair or deceptive acts or practices in or affecting commerce. Generally, misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices and are thus prohibited by Section 5(a) of the FTC Act. Also, acts or practices are deemed unfair under Section 5 of the FTC Act if they cause, or are likely to cause, substantial injury to consumers that consumers cannot reasonably avoid themselves, and that is not outweighed by countervailing benefits to consumers or the competition. The FTC has acted in multiple cases involving data security and conducts a wide range of investigations into privacy practices across industries. The FTC does not regulate everyone, as they have no authority over non-profits or the insurance industry, but they do cover a wide range of industries and companies.

How does Privacy Law impact Security professionals?

Privacy issues increasingly impact virtually all companies in all industries. Security professionals can help implement privacy laws in multiple areas.

Overall Compliance

Privacy compliance usually requires effective information security controls. Information Technology resources are increasingly relevant for individual privacy rights, such as the right to access or delete personal information.

Litigation

Personal data is becoming entwined in a growing range of litigation. Security professionals are often required to gather, retrieve, analyze, and evaluate this personal data in connection with litigation.

Mergers and Acquisitions

Privacy and security compliance is now a first-tier business issue in mergers and acquisitions. Companies interested in acquisitions, investments or other business partnerships are spending significant resources to evaluate the privacy and security practices of their targets, and are making decisions based on whether the businesses they are scrutinizing have effective security, strong privacy management, data rights, and a broad range of other areas critical for these transactions.

Product Design

"Privacy by Design" is an increasingly important concept that means that privacy controls and effective security practices need to be built into products. This integration needs to start during the design phase; it can no longer be assessed at the end of the product development lifecycle. Additionally, because of the sector-specific nature of most US laws today, companies need to evaluate data-flows, and other data-gathering efforts (for both privacy and security) to assess which set of laws is applicable to company activities.

Corporate Strategy

Companies are assessing data issues as a key element of corporate strategy. Aside from questioning which laws apply where data assets are now a critical corporate asset. Companies must evaluate data rights, the ability to exchange data, effective security activities, and a broad range of data exchange issues as key elements of corporate strategy.

> "Your role is critical and can be directly useful to the company's success in its overall business activities."
>
> - Kirk Nahra

Business Relationships

Companies have begun incorporating privacy and security considerations into their general business relationships. This includes service providers, other business partners, and situations where the company itself is a service provider to its clients. All of these activities involve data security issues and overall privacy assessments.

Marketing

Privacy laws often target marketing practices. Companies need to evaluate technical data-flows, data exchange with partners, and an overall approach to marketing, along with effective controls, to ensure that critical information is not the subject of data breaches. Marketing profiles of consumers now involves detailed and sensitive information, and they must be protected from unauthorized access.

Thinking About Vital Security Issues

As you think about how you best can partner with your privacy, colleagues, also think about these key areas. Your role is critical and can be directly useful to the company's success in its overall business activities.

Validation of Data-Flows

As the Internet of Things expands, companies are collecting data through new technologies without necessarily knowing or planning for it. Effective security controls are critical if companies want to ensure that their data collection is appropriate, targeted within existing rules and consistent with the company's obligations and interests. At the same time, this effort needs to include an evaluation of data sources. Where are outside data coming from? Do those partners have the appropriate permissions and rights to the data?

Consideration of Sensitive Data Categories

While a growing range of laws protects all forms of personal information, not all personal data is the same. Many laws create categories of "sensitive" data, and the impact of certain sensitive data clearly carries greater risks for companies in the event of a privacy or security breach. Security professionals should work with their companies to assess situations where sensitive data are collected and stored, to ensure this data is appropriately protected. Sensitive data categories clearly include health and financial information, but also genetic information, biometrics, facial recognition, and location data (and part of what makes data sensitive is how it can be combined with other data).

> "An effective partnership with company privacy officials is critical to appropriate protection of companies, their employees, their customers and any other individuals whose data is being collected by these companies."
>
> - Kirk Nahra

Aggregation

Companies need to evaluate whether they are permitted to aggregate data for purposes such as analytics or product improvement and often need technical and security assistance to ensure that data can effectively be integrated if permissible. A related question is whether a company is permitted to legally or practically de-identify data, which often expands the permitted uses of

that data. However, security professionals should keep in mind that this also creates security risks if the data is accessed inappropriately.

Data Usage

Companies need to assess how their data is being used, both internally and externally. Security professionals are critical to understanding both internal and external data flows as well as assisting with effective controls. This ensures that data usage is consistent with company strategy and legal obligations.

Client Relationships

As part of these data rights issues, companies are evaluating what their rights are when a client relationship ends. This involves a combination of legal and contractual rights, as well as the ability to locate, isolate, and manage client data. An effective “termination” approach usually requires the input of a security professional.

The Future of Privacy Law

Privacy and data-security law are still in their infancy. In the US, this field is barely 20 years old. At the same time, the law is evolving at an incredibly rapid pace, creating ongoing, changing obligations in real-time for virtually all industries across the globe. We can expect this evolution to continue, likely with the addition of other state "overall" privacy laws, potentially including a US national privacy law in the next few years. As the types of personal data grow and the range of companies that gather, collect, and analyze personal data expands, it will be critical for privacy and security professionals to work together to provide appropriate business strategies and effective protections for both companies and consumers. While these issues may seem daunting, building effective partnerships between security, privacy, and legal colleagues will provide businesses with the necessary background, information, and support to effectively guard the personal data of their clients and consumers.

About the Author

Kirk J. Nahra is a partner with WilmerHale in Washington, D.C., where he co-chairs the Cybersecurity and Privacy Practice. He teaches Health Care Privacy and Security Law and Information Privacy Law at the Washington College of Law. He is an adjunct professor at Case Western Reserve University Law School and the University of Maine Law School. He also serves as a fellow with the Cordell Institute for Policy in Medicine & Law at Washington University in St. Louis and as a fellow with the Institute for Critical Infrastructure Technology. He can be reached at (202) 663-6128 or kirk.nahra@wilmerhale.com. Follow him on Twitter @kirkjnahrawork.

About ICIT

The Institute for Critical Infrastructure Technology (ICIT) is a 501c(3) cybersecurity Think Tank with a mission to cultivate a cybersecurity renaissance that will improve the resiliency of our Nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders.