Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 14, NUMBER 8 >>> AUGUST 2014

Privacy and Data Security Laws in the U.S.: Key Elements and Practical Steps for Companies' Compliance

By Kirk J. Nahra, of Wiley Rein LLP, Washington, a member of Bloomberg BNA's Privacy & Security Law Report Advisory Board.

"Privacy and data security law in the U.S. is sector and practice specific."

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 the front page).

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.

In the mid-1990s, "privacy" began to develop a new identity, 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 EU Data Protection Directive was adopted in 1995 and still dominates much of the privacy policy debate today. As the Internet era began, the U.S. 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 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 (HIPAA) 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. 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. This article focuses 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 applies only to companies that have customers or employees.

Starting with the BJ's Wholesale case in 2005,[1] the Federal Trade Commission (FTC) 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 is currently being challenged in cases involving Wyndham Hotels 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; and
- evaluate and adjust its 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.

These obligations are detailed, often overlapping and complicated, and create ongoing risks for litigation, business disputes and government enforcement.

Cybersecurity

The latest security add-on is the ongoing debate about cybersecurity. The federal government—led by the White House—is making an improved overall industry posture on cybersecurity a significant priority, to protect national security as well as personal data. Although the obligations (at this point) are less specific, there is an ongoing push for specific cybersecurity legislation, with developments on a daily or weekly basis.[2] At the same time, the administration is implementing a series of programs stemming from a 2013 Executive Order that will expand overall protections for cybersecurity. Although these provisions focus (to date) on "critical infrastructure" industries, these steps should be important considerations for any company, because of the focus on ongoing company operations related to cyberspace and the Internet.

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 article is not the place for a full evaluation of HIPAA's detailed requirements,[3] but companies must consider HIPAA's requirements if any of these categories apply to them:

   ISSN 1473-3579

- 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 that contract with companies in the health care business (and onward downstream indefinitely); or
- 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 which may not be aware of their responsibilities.

Website Privacy Policy

For any companies that operate a website, 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) meet 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.[4]

Telemarketing/E-mail Marketing

Another key area of privacy regulation for most companies 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 signed up in droves for do not call registries. These issues affect only companies that conduct telemarketing. For them, this is a big deal.

On a broader level, the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM), which deals with e-mail marketing, has a broader application to a wide range of companies.[5] 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 adopted its own version of CAN-SPAM, which requires more aggressive front-end consent from individuals, key parts of which entered into effect July 1, 2014[6] (*see analysis at WDPR, May 2014, page 19*). If a company engages in any activity that could be construed as marketing through e-mail, 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.[7] 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[8]) 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.

There are certain relatively common terms to these state breach notification 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.

Practical Steps

So, what do companies need to do about these laws?

Although companies vary in their knowledge of and planning for these obligations, here are some key steps to consider regardless of the level of regulation or preparation:

Does the Company Know What Kind of Information It Has and What Happens to It?

This article focuses on laws and regulations that are generally applicable. However, each company has its own privacy/data security risk profile, based on the industries it works in, the kinds of data it has and the businesses to which it provides services. Every company needs to think about the information it has and what it does with it, as a starting point. These steps include:

- evaluating any place that a company collects, stores and discloses sensitive data (especially Social Security number and credit card information—**this review of Social Security number usage is the single biggest risk reduction step a company can take**);
- paying attention to employee data as well as customer data; and
- identifying where this information is disclosed.

Is the Company Paying Attention to the Right Rules?

Then, once a company has a sense of the personal data it gathers, it must think about the regulatory requirements for this information and for the business. Questions for the company to ask include:

- Is it following the various marketing rules?
- Does it collect information from children online?
- Has it thought about any health care benefits program?
- Is it disposing of sensitive information properly?
- Has it told employees how it monitors them?

Does the Company Have an Appropriate Information Security Program?

Moving beyond privacy issues, companies then must turn to the generally applicable principles regarding information security. These steps are both required by enforcement practices (for all industries) and detailed legal requirements (for certain industries), and protect companies against lawsuits, customer complaints and business disruption. In thinking about information security, a company should ask the following questions:

- Is someone assigned this responsibility?
- Does it have documentation for a regulator?
- Does the program encompass paper and electronic information?
- Has it trained employees on basic information security?
- Does it have appropriate contracts and oversight of vendors?

Is the Company Ready to Act if There Is a Problem?

All of these proactive steps are designed, at least in part, to reduce the likelihood of an actual problem. One key element of protecting a company is to make sure that, if a problem arises, it is prepared to act quickly, to reduce potential harm and protect the company and its customers as much as possible. In considering these issues, companies should ask the following questions:

- Does it know who is in charge?
- Do employees know where to go in the event of a problem?
- Does it have a good program to identity and fix problems?
- Has it evaluated the requirements for security breach mitigation and notification?
- Has it considered whether cyber insurance or other data breach insurance is a good fit?

Companies Must Understand with Whom They Have Business Relationships

Last, beyond thinking about its own business activities, companies also need to think about their business partners, both their own customers and their service providers. Effective compliance is a legal requirement and a business imperative in dealing with potential customers, too. For a company's own vendors, service providers create significant risk and must be overseen effectively. A company must think about the following:

- assessing its role as a vendor and as a company that hires vendors;
- developing an "offshoring" approach;
- developing a realistic vendor approach for due diligence, oversight, monitoring and contracting that, for the most part, is "one size fits all"; and
- making sure employees are aware of these responsibilities—and don't take on too much or give away too much.

Final Thoughts

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 gen-

   ISSN 1473-3579

eral 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.

NOTES

[1] *See* Federal Trade Commission, *In the Matter of BJ's Wholesale Club, Inc.* (last updated Sept. 23, 2005), *available at* http://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter.

[2] See http://www.nist.gov/cyberframework/index.cfm for recent developments related to cybersecurity standards across these "critical infrastructure" sectors.

[3] For a primer on HIPAA compliance, see Kirk J. Nahra, *HIPAA Privacy and Security for Beginners*, PRIVACY IN FOCUS (July 2014), *available at* http://www.wileyrein.com/publications.cfm?sp=articles&id=9855.

[4] Online Privacy Protection Act of 2003, California Business and Professions Code §§ 22575–22579.

[5] 15 U.S.C. §§ 7701–13.

[6] Canadian anti-spam law, "An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities," S.C. 2010, c.23.

[7] The U.S. Congress also has been debating a federal breach notification law for several years. Although the Target breach in November 2013 led to additional hearings on breach notification, there currently is no generally applicable federal beach notification law.

[8] Cal. Civ. Code §§ 1798.29, 1798.80 *et seq.*

Kirk J. Nahra is a Partner with Wiley Rein LLP in Washington and the Chair of the firm's Privacy and Data Security Practice. He is a member of Bloomberg BNA's Privacy & Security Law Report Advisory Board. He may be contacted at knahra@wileyrein.com.