wiley

NEWSLETTER

Privacy and Data Security Is for Everyone

August 2014

"Privacy and data security law in the United States 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 United States that does not have specific legal obligations and risks related to the privacy and security of personal data. The details may change, depending on your industry and your 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.

Through the passage of dozens (or, more accurately, hundreds) of laws and regulations at the state, national, and international levels, the sector-specific perception needs to be re-evaluated. 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 over-lapping, 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 being taken to evaluate risk and manage potential legal exposure.

What Do Most Companies Have to Worry About?

The key components of the privacy and data security universe for everyone are:

Overall Data Security

The easiest piece to start with is the obligation of every company to protect the security of sensitive personal data. Technically, this only applies to companies that have customers or employees, so your company only has to worry about these obligations if you have customers or employees.

While the FTC's requirements are not voluminous, they require ongoing activity from companies involving the security of personal data. These requirements have significant flexibility, but require a thoughtful, proactive security program that stretches across a company's full operations and keeps pace with ongoing changes in both business operations and technological evolution connected to information security.

Cybersecurity

The latest security add-on is the ongoing debate about cybersecurity. The federal government—with a focus on the White House—is making cybersecurity protections an even broader set of challenges. While 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.

HIPAA

While the focus of the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules is on the health care industry, these rules set out obligations that apply to a large number of companies across many industries. Your company must consider HIPAA's requirements if any of these categories applies to you:

- You are in the health care business as a health care provider or health plan;
- You contract with companies in the health care business (are a service provider to these health care companies);
- You contract with companies that contract with companies in the health care business (and onwards downstream indefinitely); or
- You provide health care benefits to your employees.

Website Privacy Policy

For any companies that operate a website, it 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.

Telemarketing/Email 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 one of the most successful privacy laws (at least from the consumer perspective), as individuals seem to care about these issues and have in droves signed up for the do not call registries. Additionally, the CAN-SPAM law that deals with e-mail marketing applies broadly to a wide range of companies. If your company engages in any activity that could be construed as marketing through e-mail, then you must make sure that you are complying 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. While 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 that expand the reach of these statutes.

And, since 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.

Action Items

So, what do you need to do about these laws? While companies vary in their knowledge of and planning for these obligations, here are some key steps to consider regardless of your level of regulation or preparation.

- Do you know what kind of information you have and what happens to it?
- Do you understand who your business relationships are with?
- Are you paying attention to the right rules?
- Do you have an appropriate information security program?
- Are you ready to act if there is a problem?

Final Thoughts

Privacy and data security are not going away. New laws and regulations are placed on the books regularly. Enforcement, while still modest, is growing. Litigation also is growing. And ongoing developments involving the risks and benefits of "big data" present the certainty that the complexity of this environment will continue to grow. Effective privacy and data security practices are an essential component of the business operations of any business. While the challenges may seem daunting, the most important steps are to understand your general level of exposure, and to undertake a creative, thoughtful, and thorough assessment of your privacy and data security activities, so that these growing risks can be managed effectively.

This article is excerpted from a more comprehensive piece, published by the Bloomberg BNA Corporate Law & Accountability Report on July 18, 2014, entitled "Privacy and Data Security Is for Everyone: Common Matters That All Companies Should Address." For the full article, please see http://www.wileyrein.com/publications.cfm?sp=articles&id=9895.