Privacy and Information Security for Emerging Businesses

05.11.2010

Elizabeth H. Johnson

Your business just got off the ground, or maybe it's still on the tarmac. You have to worry about recruiting new talent, marketing your products and services, securing your IP, and, most important, attracting investors. With all that to think about, why consider privacy and information security issues?

You should consider these issues for several reasons, but the prime reason is that you don't need any distractions. Two features of this area of law are poised to become major distractions: increasingly frequent government enforcement actions and information security breaches.

The FTC has taken more than 20 actions alleging that inadequate information security constituted an unfair trade practice. These actions are typically settled with the offending entity, in which settlements require implementation of a comprehensive, written information security program and a third party audit of compliance with that program every other year for 10 or 20 years. Multiple state attorneys general have taken similar actions. In addition, Mississippi has just become the 46th state to enact a law requiring businesses experiencing a security breach to notify affected individuals if their personal information is impacted. These laws mean that whether an employee lost a laptop containing Social Security numbers or your system including financial account numbers was hacked, you have a legal obligation to send letters to each person affected explaining what happened. That letter may be read with interest by regulators, plaintiffs' attorneys, the media, and, unfortunately, potential investors or customers. Whether you're responding to government enforcement or containing a security breach, productivity and cash flow will both be adversely affected.

Developing a comprehensive approach to privacy and information security will help avoid these potential distractions, minimizing the risk of both enforcement and a breach. Depending on your business model, you may have additional compliance considerations to incorporate in your approach.

As you develop that approach, keep in mind the following considerations relevant to any emerging business:

Start Now

It will be much easier to design and implement a privacy and information security compliance program now while you are small and nimble. As your organization grows, so will the quantities of information you maintain and the diversity of practices your employees use to manage that information. Changing the process midstream and teaching them compliance after their potentially bad behaviors have developed are much more difficult.

Consider It a Selling Point

Risks in this area are increasing exponentially. A reportable security breach drains productivity and can bring bad press and unwanted attention from regulators. That, in turn, diminishes your organization's potential value as an investment or acquisition target. Whether or not you have an incident, a potential investor or purchaser may simply consider it a plus that your organization has a privacy compliance program. They may even decide to leverage it for their own business use.

Consider Your Business Model

Are you developing a system to track and report on consumers' behavior and preferences to inform marketing campaigns or product development? Are you deploying a "cloud computing" solution that will allow multiple, disparate businesses to outsource data hosting or software management to your organization? Or is your goal to develop a mobile device that will facilitate more efficient use of electronic health records by health care providers? These and countless other examples involve business models that have, at their core, significant privacy and information security compliance and risk considerations. The best way to avoid having your success stifled by existing privacy requirements is to build a program that addresses these issues now, one that is flexible and scalable for future growth.

Consider Your Future Business Model

If you currently send direct marketing materials by email, consider how your compliance obligations will change if you start sending text messages as well. Getting into e-commerce? Want to reach out to consumers in international jurisdictions? To kids under 13? All these business models will raise privacy obligations that could be anticipated and incorporated into your approach in advance so that you don't have to adjust your practices later to accommodate the legal requirements.

Consider Your Back-Office Functions

Even if your front-end business does not involve personal information or the types of technologies that make privacy compliance a concern of primary importance, your back-office functions will give rise to privacy compliance issues. For example, paying employees and providing them with standard benefits means you also are responsible for managing personal information in their personnel file, ensuring that your employee welfare benefits plans are HIPAA-compliant and including appropriate contractual protections in any agreement with vendors that manage functions such as payroll that involve employee personal information. Other concerns may include conducting background checks, monitoring employees' use of information systems or the Internet, or developing a comprehensive records management program to address the volumes of files your business will shortly commence to generate. Whatever the privacy issue, anticipating these considerations and addressing them at an early stage will be more efficient and cost-effective than they will be years down the road when implementation will mean changing existing practices.

In order to develop a comprehensive, scalable, forward-looking privacy compliance program, you need legal representation from attorneys who take a comprehensive approach to these issues. Our privacy and information

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075

security attorneys practice in all areas of this topic, from CAN-SPAM to HIPAA, from security breach to European data protection law, from online privacy to records management.

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075