The Privacy Puzzle

As the privacy debate heats up, FTC Commissioner Julie Brill is emerging as a key player in U.S. and global regulations.

By Erin E. Harrison, InsideCounsel

December 22, 2014

FTC Commissioner Julie Brill, photo by Tony Powell

Amid a growing list of high-profile data breaches in the United States and increasing concern by consumers over a lack of privacy, Congress will reconvene this month having not yet passed a major cybersecurity bill. The lack of overarching regulations has left many organizations with little help to define their cybersecurity strategies, and has led (in)2(e)6(l(e)-3(t)-P <<>>BDC 0te)-4(g)-4

Disruptive trends in data security

Businesses today face a myriad of issues related to the confluence of data security and privacy, but there are three specific trends Brill sees when it comes to shaping the privacy agenda for companies. They are: the so-called Internet of Things, third-party data brokers and information pertaining to financial or other sensitive subjects changing the way business is conducted, and as a result, accelerating concerns about data protection.

“Some of them involve sensitive data, home life and where we are moving on a minute-to-moment basis with location-based information,” Brill explains. “My primary concern is data security; 90 percent of connected devices collect personal information and 70 percent are not encrypting that data. It's a big concern. Businesses need to be aware this is happening, if they are part of this ecosystem and active in one or more of these areas in the ecosystem.”

In the Internet of Things, appliances, medical devices, wearable technologies and even vehicles are networked, collecting information about users that could help to predict preferences or product needs. While the Internet of Things presents potentially exciting opportunities for customers/end users, businesses also face a greater accountability level to ensure they are properly protecting consumer data and other sensitive information.

Just as impactful on information policy, are data brokers, key players in a multi-billion dollar industry that collects, analyzes and sells the personal information of millions of Americans. They need to be closely watched regarding how they are using that data and whether they are providing enough transparency.

Rounding out the disruptive trends in the space is the collection of sensitive information.

The impact of this will vary considerably depending on industry, however, security measures concerning health and financial information have received considerable focus by regulatory bodies, which will likely impact the way other types of sensitive information will be controlled as well.

“The ways in which health information is flowing now throughout our digital lives are much broader than what was captured in laws adopted a couple of decades ago (such as HIPAA.) If you are online and searching for information about a disease, or on an app, your information is not necessarily protected by HIPAA,” explains Brill. “The question is: are we appropriately protecting all of this health information, including the information generated through these technologies? Companies need to more attuned to this issue if they are collecting or using health information generated in these new ways.”

As stated earlier, the volume of sensitive information varies by industry, as does the reliance on data brokers and the proximity to connected devices. That being said, one prevailing thread among all three trends is Big Data, the increasing predilection to collect large volumes of information for predictive analysis.

“We need to think about how to structure a framework for companies to determine whether their Big Data projects are appropriate. In addition, we need to think about collection too: how much data is being collected and whether that specific data is needed. Unbounded data collection can lead to data security problems if the data is not appropriately de-identified,” Brill points out. “The other thing we need to think about in the context of a framework focused on data use: who will participate in the decisions about appropriate and inappropriate uses?”

FTC initiatives

In the past couple of years, the FTC has embarked on a number of initiatives to lead the charge toward more stringent privacy and data security standards, expanding its authorities under Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive acts or practices against consumers. Last year, the FTC brought 53 data security enforcement cases and over 40 privacy cases that addressed personal information.

There has also been a surge of activity focused on developing guidelines, and businesses and consumers alike have a lot to say when it comes to privacy protection. The FTC regularly holds public workshops on emerging issues to generate public discussion and develop best practices to help businesses steer clear of anything close to inappropriate activity. The Commission has also taken a proactive approach to educating businesses on their responsibilities under different laws; the agency has also taken a consumer-facing tack toward education to help end users make wiser choices and be aware of the potential risks of sharing their information.

There are five core components that make up effective data security practices, according to the FTC, which Brill broke down as follows:

“One, conduct risk assessments of the data your company has and what could happen if the company were to suffer a breach; two, minimize personal information about consumers, de-identify as much as possible and don't pass the information along to companies that will try to re-identify; three, implement technical safeguards, such as encrypting personal information as appropriate, and also protect the physical systems that store personal information; four, train employees to handle personal information properly; and five, put a breach response plan in place so if the company does suffer a breach, there is a plan for how to deal with it.”

These points provide a basis for how to effectively operate within the FTC matrix of regulations. Brill says that adherence to these practices can protect companies even when they've been the victim of a data breach.

“When we are doing an investigation, we are often looking at whether a company has failed to maintain reasonable security such that they cross the line of an ‘unfair practice’ under Section 5 of the Federal Trade Commission Act. But just because a company suffers a security breach doesn't meant they failed to maintain reasonable security and doesn't mean they broke the law,” Brill says.

Mitigating risk

While there is no silver bullet to ensure businesses will avoid a data breach altogether, the C suite and the board have a mandate to create and maintain measures designed to protect operational data as well as sensitive information concerning employees and customers.

“The most important thing for a company to do is to begin viewing privacy and personal data as risks to a company's reputation as well as its financial well-being. More and more companies are taking this view,” says Brill. “The flipside of looking at these privacy and data security issues as both reputational and financial risk is focusing on engendering consumers’ trust. Engaging in these conversations in the C suite is one of the ways GCs can bring these issues and perspectives up to the top and then get this message to spread throughout their companies.”

Aside from the various enforcement trends and policies general counsel need to be thinking about, the C-suite as well as the board of directors are charged with ensuring that basic consumer protection principles apply to new technologies. For companies that are currently developing plans to integrate data privacy and compliance, Brill recommends thinking of privacy as a compliance matter and to proactively consider the risks involved. This includes thinking about privacy issues during the development phase of new products and services, rather than after the fact.

“This will raise the profile of these issues if you are thinking in those terms. One of the things we are asking companies to do is to think about privacy by design. That is, don't wait until you have a problem, but instead, incorporate privacy at every stage of development. Think about it from the beginning, not just at the end.”

With their ability to enact steep fines and