THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp

Illinois AG Targets ID Theft, Earlier Breach Notification

By Divonne Smoyer, CIPP/US*
Christine Czuprynski**

April 28, 2015

Illinois Attorney General Lisa Madigan

Illinois Attorney General (AG) Lisa Madigan has spent the last decade focused on consumer privacy and data security issues, from the passage of data breach legislation in 2005 to her testimony in front of Congress earlier this year on federal data breach legislation. Her office established its Identity Theft Hotline in 2006 to address specific consumer complaints, and she has participated in multistate data breach investigations of the most high profile breaches. Madigan talks to *The Privacy Advisor* about what has changed since 2005 and how her office is responding.

The Privacy Advisor: You recently testified before Congress regarding whether this country needs a federal data breach notification law and argued that a federal law is needed but only one that does not preempt more restrictive state laws. Why do you think a federal law is a good idea? Will individuals and businesses both benefit from a uniform federal law? Why do you feel it important that any preemption provide a "floor?"

Madigan: Since 2003, the states have acted to protect consumers from the financial and privacy risks that accompany data breaches. We passed our law in Illinois in 2005. Today, 47 states have data breach notification laws that ensure that consumers know when their personal information has been compromised. These laws have improved data security in the U.S. and brought much-needed attention to the harm that breaches can cause.

At the same time, I do believe that a strong, federal law on data breach notification would be beneficial for consumers because the federal government should play a role, and currently it has little authority to do so. Three states do not have a data breach notification law, leaving those consumers without any protection in the event of a breach. In my experience, consumers are best protected when the states and the federal government are working together to protect them. And currently, the states are largely on their own with breach notification.

Yet, such a law should not come at the expense of the important role the states already play. The states are on the front lines of data security and are in the best position to recognize insufficiencies in the law; to recognize new trends in data collection and data breaches, and to update the law. States need the ability to protect their residents from new threats as they arise. For example, various states have expanded the definition of personal information beyond financial information and Social Security numbers. If states are unable to continue this innovation, consumers will suffer from a stagnant law.

The Privacy Advisor: Identical bills have been introduced in the Illinois House and Senate that make significant changes to the Illinois Personal Information Protection Act, the state's data breach notification law. Significantly, the bills seek to amend the definition of "personal information" under the current breach notification law to include consumer marketing information, geolocation data, health insurance and medical information and biometric data. The bills also seek to require notification directly to your office within 14 business days of discovery of a breach affecting 100 Illinois residents.

Why do you see a need to amend the definition of "personal information?" How have things changed since the law was first enacted in 2006? Why do you think it is important that your office be notified in such short order following discovery of a breach or notification to residents? What kind of information will be available to the public on the Illinois breach notification website?

Madigan: Since the Illinois Personal Information Protection Act (PIPA) was enacted in 2005, the nature of data sharing and collection in the U.S. has changed; consumers are sharing much more information about themselves online, and companies are collecting very specific details about consumers' online activities. Data breaches are also becoming bigger and happening more

frequently. All of this means that sensitive details about consumers' lives are at greater risk than they were before.

This change is the impetus for the expansion of the definition of personal information. When PIPA was enacted, the goal was to prevent identity theft resulting from the exposure of personal financial and identifying information. Today, we know that other types of information—not just financial information and Social Security numbers—can expose consumers to identity theft and other harm.

Health insurance and medical information can be used to commit medical identity theft, which occurs when someone receives medical treatment under someone else's identity. Biometric data is increasingly used for authentication to access financial accounts and electronic devices. Geolocation data can expose someone to stalking or harassment or reveal intimate details about individuals like the churches they attend, the types of doctors they visit and the businesses they frequent. If companies are going to collect this sensitive and potentially harmful information, they have an obligation to protect it from disclosure and to notify consumers when it has been breached.

Earlier notification to my office is a way to improve transparency of breaches. Not only can we be prepared to help consumers whose information has been compromised, but we can also make sure that entities are not unreasonably delaying notification to consumers. The website that I envision for Illinois data breaches will be a clearinghouse for consumers to learn about breaches that have occurred. It will list the time frame of the breach and the type of information that was compromised. This idea comes directly from the interactions I had with Illinois residents at more than 25 roundtables last year. I repeatedly heard from consumers that they did not know where to find information about breaches, and they wished that there was one place where they could learn about which companies, nonprofits or government agencies had suffered breaches.

The Privacy Advisor: The bills proposed to amend the Personal Information Protection Act also seek to add a new element to Illinois law—a requirement that website operators post privacy policies on their websites that disclose the type of information collected, the disclosure of that information to third parties and how the website responds to do-not-track signals, among other things. Such a requirement currently only exists in California. Why do you think privacy policies are valuable to Internet users? Do you think it is important to go a step further than the California requirements and require website operators to respond and honor do-not-track signals?

Madigan: For consumers to make an informed decision about whether they want to use a service that tracks their online activity or whether they want to provide sensitive information to a website, the company's data collection and sharing practices must be transparent. It is unreasonable to expect consumers to hand over personal information to websites without explaining how that information will be stored, shared and used. If a consumer is concerned about how the information might be used, a privacy policy is the best way for them to make an informed decision.

Do-not-track signals are an incredibly useful way for companies to respect the privacy preferences of their customers, which is why I included language referencing do-not-track signals in the privacy policy disclosure requirements of the bill. Currently, Illinois does not have the same protections as California residents do with respect to disclosure, and I am working on adding those protections. At this point, we are not addressing what website operators should be required to do with do-not-track signals.

The Privacy Advisor: President Barack Obama spoke to the Federal Trade Commission on January 12 and announced a forthcoming bill, called the Student Digital Privacy Act, to protect the confidentiality of student data. Noting that technology and innovation in the classroom are a benefit to students, Obama then emphasized that the current regulatory environment does not adequately protect students. You have worked to protect students from other forms of fraud and deceptive practices. Do you agree with the White House that student data is deserving of special protection? Will you follow the lead in states like California and Colorado and pursue legislation at the state level that restricts the way website operators and their third-party vendors can use student data?

Madigan: Student data deserves special protection. Personal information about minors is particularly sensitive because minors are less able to protect themselves from the harms of identity theft. While technology is becoming an increasingly useful tool for educators and schools, those tools should not come at the expense of our students' privacy.

State laws that restrict the use of student data by website operators are one method for protecting children when they are inside the classroom. I have watched the development of these state laws and proposals that have been introduced in Illinois take similar steps. My office is currently working on updating the Personal Information Protection Act and has not drafted a bill on student privacy. However, it is an important topic. If needed, I will certainly consider it in the future.

The Privacy Advisor: Connecticut AG George Jepsen has recently established a Privacy and Data Security Department in his office. The president of the National Association of Attorneys General, Mississippi AG Jim Hood, has made protecting digital lives his presidential initiative for 2014-15. Other AGs are seeking to amend their data breach notification laws. Why are state AGs so focused on privacy and data security? What privacy issues, beyond data breach notification, do you think will be of primary importance to individual consumers in the years ahead?

Madigan: State AGs have focused on privacy and data security issues for more than a decade because of the growing use of the Internet and technology and because the increased use of these innovations has resulted in an expansion of data collection.

Consumers are concerned about privacy and data security as well. In 2006, I established the nation's first Identity Theft Hotline to help consumers who have become victims of identity theft and to provide information on how to prevent identity theft in the first place. So far, we have helped remove more than $27 million in fraudulent charges for more than 37,000 Illinois residents. In 2014 alone, my office received more than 2,618 complaints regarding identity theft. At the roundtables I held last year, consumers overwhelmingly wanted to know what steps my office was taking to protect their personal information. Consumers understand that their personal information—and its security—is linked to their own financial security. Identity theft is consistently among the highest categories of complaints that my office receives every year. As data collection and national breaches become more prevalent, consumers will be more focused on its implications as well.

The rapid pace of technological innovation has led to some amazing new uses and sources of consumer data. From fitness trackers to the Internet of Things, consumers have access to a wide range of data-driven products. Many of these products, however, will have the ability to collect sensitive information about consumers, sometimes without the consumer understanding the implications.

Biometric data and health information, for example, can be collected from fitness trackers. If this information were shared by the data collector with data brokers, it could be used to develop a profile about the consumer. Both the FTC and the U.S. Senate Committee on Commerce, Science and Transportation have released reports warning about the potential harm that these profiles can cause consumers. If consumers are identified as having diabetes, cancer or HIV, they could be discriminated against, targeted for predatory financial products or pay higher insurance costs. The risk of personal information being collected from these products and used for negative purposes is real and will likely be an area of consumer concern in the future.

***Divonne Smoyer**, CIPP/US is a partner at the Reed Smith LLP in Washington, DC, where she specializes in legal and policy matters involving state attorneys general and consumer protection, including in the areas of cyber security and data privacy. She frequently writes and speaks on privacy issues and reforms, and is a member of IAPP's Education Advisory Board. Smoyer is a CIPP/US and a graduate of Smith College, summa cum laude, and Harvard Law School, cum laude.*

***Christine Czuprynski** was an Assistant Attorney General in the Consumer Fraud Bureau of the Illinois Attorney General's office where she handled privacy matters. She now works in the Chicago office of Reed Smith LLP and handles data privacy and security legal matters.*