Prepared Statement
Illinois Attorney General Lisa Madigan
"Getting it Right on Data Breach and Notification Legislation in the 114th Congress"

Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security
Committee on Commerce, Science, and Transportation
United States Senate

February 5, 2015

I. Introduction

Chairman Moran, Ranking Member Blumenthal, and members of the Subcommittee, thank you for giving me the opportunity to speak with you. Data security is one of the biggest challenges we face in the United States today. It is an ongoing struggle for companies, non-profits, government agencies, and consumers.

While last year's massive data breaches were a national turning point for public awareness, this is not a new problem. For over a decade, my office has been investigating major data breaches and helping consumers respond to identity theft.[1]

In 2005, we passed a data breach notification law in Illinois to ensure consumers are notified when an entity suffers a breach of their sensitive personal information. And in 2006, I created an Identity Theft Unit and Hotline to help consumers restore their credit when their information was used without their authorization. So far, we have helped remove over $27 million worth of fraudulent charges for over 37,000 Illinois residents.[2]

[1] Since 2006, identity theft and data breaches have either been the most common complaint, or the second most common complaint, received in the Illinois Attorney General's office. Only complaints related to debt have had a higher total.

[2] In 2014, the Illinois Attorney General's office received 2,618 complaints regarding identity theft and helped return over $918,000 to consumers who suffered identity theft.

At this point, everyone knows it is not a question of if they will be a victim of some form of identity theft, but when. Because at every hour of every day, any entity that maintains a database of sensitive information could be under attack.

The economic impacts have been, and will continue to be, enormous. Everyone agrees that we need to do something. Everyone wants to prevent data breaches. And everyone wants to prevent identity theft. The question is—how do we best do this?

I have long supported the push for a national law on data breach notification. In 2005, I joined forty-three other state attorneys general to call for a national law on breach notification,[3] so I am heartened that Congress looks poised to pass a law. But simply passing a law that replicates state laws will do very little to protect consumers that is not already being done.

Congress must move beyond a debate about data breach notification. For the most part, we already have data breach notification in this country. Forty-seven states have passed laws requiring companies to notify consumers when they suffer data breaches. Many states have either passed, or are working to pass, a second or third-generation version of their laws.

II. The Need for Transparency

We need more transparency on data breaches and data security, not less. We should not hide from the fact that our data can be compromised, and we should not hide data breaches when they occur. I have recently heard an argument that consumers are experiencing data breach fatigue, and that additional notification may be counter-productive. I strongly disagree.
In my experience, consumers may be fatigued over data breaches, but they are not asking to be less informed about them.

[3] Letter to Congressional Leaders from the National Association of Attorneys General (NAAG) (Oct. 27, 2005).

Last year, I held over twenty-five roundtables on data breaches throughout Illinois, with nearly 1,000 Illinois residents from all walks of life—law enforcement officials, small business owners, consumers, and senior citizens.

Here is what they told me. When their information is stolen, they want to know. They also want to know what they can do to protect themselves from identity theft and data breaches. And they want to know whether entities are doing enough to protect their information and prevent breaches.

Unfortunately, my office's investigations have revealed that entities have repeatedly failed to take basic data security precautions. We have found instances where entities:

- allowed sensitive personal data to be maintained unencrypted;
- failed to install security patches for known software vulnerabilities;
- collected sensitive data that was not needed;
- retained data longer than necessary; and
- failed to protect against compromised login credentials.

Understanding where data security failures occur is what leads to data security fixes. Without transparency, data breaches and their causes will remain hidden. Notification also allows consumers to take steps to protect themselves following the aftermath of a breach. This transparency is not possible without laws mandating it.

III. Information that Triggers Notification

Therefore, Congress should pass a data breach notification law that covers the growing amount of sensitive personal information that entities are collecting. Any definition of protected "personal information" should be broad, and the Federal Trade Commission should be given the

power to update the definition as needed. It is not just stolen social security numbers or stolen credit card numbers that consumers have to worry about now.

When I first worked to pass a law in Illinois on this issue nearly a decade ago, we were focused solely on protecting consumers against identity theft and fraud.[4] In the intervening ten years, the Internet has grown more than we imagined possible. This growth has been great for our economy and it has made our lives easier. But it has also made individuals more vulnerable to data breaches because more entities are collecting increasingly specific data about them. Any law designed to protect consumers should reflect this fact.

Congress should seek to pass legislation that ensures notification of breaches related to pieces of information that can do us any kind of harm, whether that is financial harm or reputational harm. For example, this kind of data includes:

- login credentials for online accounts;
- medical information shared on the Internet that is outside the scope of the Health Information Technology for Economic and Clinical Health (HITECH) Act;[5]
- biometric data; and
- geolocation information.

The recent attack on Sony was a lesson for all of us. Reputational harm can be far worse than financial harm. It can hurt companies, and it can destroy lives. In Illinois, I will be seeking to

[4] Illinois Personal Information Protection Act, 815 ILCS 530/1 et. seq. The Illinois Personal Information Protection Act requires notification to Illinois consumers in the event of a data breach. A breach is the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of "personal information." Currently, "personal information" is defined as an individual's first name (or first initial) and last name combined with any of the following: social security number; driver's license or state identification card number; or account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

[5] Title XIII of the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5.

update our law to protect the type of data about individuals that entities are regularly collecting, and I encourage the Subcommittee to do the same.

IV. A "Harm Analysis" Hurts Consumers

Next, an entity should not be conducting a "harm analysis" to determine whether it should notify consumers about a data breach. If an entity holds our sensitive information and loses it, most people want to know. The very loss of sensitive personal information should be viewed as harmful generally, and it is nearly impossible to truly determine what specific harm may or may not occur following a breach.

Imagine if a landlord learned that a renter's home was robbed and that landlord had the opportunity to decide whether the stolen items were significant enough to let the renter know about the robbery. We are considering allowing this for stolen data with a so-called "harm analysis." It will not lead to better data security, only fewer breach notifications.

V. Federal Role in Data Security

Finally, data breach notification alone, no matter how expansive, will not be enough to secure our data. Congress also needs to ensure entities holding sensitive information are taking reasonable steps to protect that information. To do that, it should require companies to implement reasonable security standards and it should give the Federal Trade Commission the authority to promulgate regulations as needed.

Congress should also focus its attention on the current authority of the federal government to investigate massive data breaches that affect millions of Americans. When such breaches occur, the federal government should have the general authority to investigate in the same manner the National Transportation Safety Board (NTSB) can investigate accidents. Currently, the federal government has no such authority. Federal law enforcement agencies can

conduct a criminal investigation to determine who was responsible for an attack, and the federal government, through the Federal Trade Commission and other agencies, can conduct an investigation to determine whether the entity's data security practices were adequate. However, no federal agency is tasked with simply uncovering what happened in massive data breaches, regardless of whether an entity's data security practices were adequate.

If a federal agency had this authority, that federal agency would develop much-needed expertise in data security. It could issue reports about data breaches so that the private sector would better understand what vulnerabilities led to breaches. Our country would also have a much better sense of the general state of our data security.

VI. Role of the States

I understand that Congress will consider preempting states on data breach notification laws. As a state official, I oppose any federal legislation that limits our ability at the state level to protect our residents. In 2005, along with forty-three other state attorneys general, I wrote to Congress to caution against broad preemption.[6] In the letter, we wrote:

> Preemption interferes with state legislatures' democratic role as laboratories of innovation. The states have been able to respond more quickly to concerns about privacy and identity theft involving personal information, and have enacted laws in these areas years before the federal government. Indeed, Congress would not be considering the issues of security breach notification and security freeze if it were not for earlier enactment of laws in these areas by innovative states.[7]

In the decade since we wrote that letter, it has become clear that preemption would have been a mistake for consumers.

Additionally, a narrow view of preemption has been adopted in other federal data security laws. The Gramm-Leach-Bliley Act (GLBA), which established data security standards for

[6] Letter to Congressional Leaders from the National Association of Attorneys General (NAAG) (Oct. 27, 2005).

[7] *Id.*

financial institutions, only preempts those state laws that are inconsistent with federal law and "then only to the extent of the inconsistency."[8]

Similarly, in 2009, Congress took a narrow approach to preemption in the breach notification provisions in the Health Information Technology for Economic and Clinical Health (HITECH) Act.[9] That law imposes the HIPAA preemption standard, which only preempts contrary provisions of state law.[10] For those laws that protect the privacy of individually identifiable health information, the HIPAA Security Rule goes even further, to save any state law that is more stringent than the HIPAA protections.[11] Together, these provisions illustrate a reasonable and workable approach to preemption. If Congress does preempt the states, for the benefit of consumers:

- the law should be a "floor" with a narrow preemption provision;
- the law should preserve a state's ability to use its consumer protection laws to investigate data security practices; and
- states should have the right to enforce the federal law.

VII. Conclusion

The roundtables on data security that I convened throughout Illinois last year showed me that data breach notification is working. Consumers are well aware of data breaches generally. But one challenge is making sure the affected consumers learn about the right breaches.

[8] 15 U.S.C. § 6807(a).

[9] Title XIII of the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5.

[10] 42 U.S.C. § 1320(d-7).

[11] 45 C.F.R. § 160.203.

Understandably, in certain circumstances, state laws allow companies to comply with notification requirements by notifying the media.[12] Bills being considered in Congress allow similar notification exceptions. But the most often comment I received during these roundtables was that consumers did not know where to go to learn about breaches. It has become clear to me that it is not enough to require companies to notify the media.

As a result, in Illinois, I am proposing a requirement that companies also notify my office when they suffer a breach. Fifteen states already require entities to notify their Attorney General in the event of a breach.[13] If given that authority, I intend to create a website that will enable Illinois residents to see all the breaches that have occurred in Illinois.

Such a website is only possible at the state level because we can include information about national breaches, as well as those that are local or regional. I believe such a service would greatly benefit Illinois residents, and I do not believe they would want Congress to prevent my office from offering it, or the other work we are doing on data security and data breaches.

I am happy to answer any questions you have.

Thank you.

[12] *See, e.g.*, Illinois Personal Information Protection Act, 815 ILCS 530/10(c).

[13] Cal. Civ. Code 1798.29(e); Conn. Ch. 669 Sec. 36a-7041b(b)(2); Fla. Stat. §501.171(3); Ind. Code Art. 24-4.9-3-1(c); Iowa Senate File 2259 (to be codified at 715C.2.8); LA Admin. Code Title 16 § 701; Maine Stat. Tit. 10 §1348(5).; Md. Comm. Code §14-3504(h); Mass. Gen. Law Ch. 93H Sec. 3(a); Mo. Stat. §407.1500(8); N.H. Ch. 359-C:20(b); N.Y. §899-aa(8)(a); N.C. Gen. Stat. §75-65(e1); Vt. Stat. Ann. Tit. 9 § 2435(b)(3); Va. Code §18.2-186.6(E).