



**U.S. HOUSE OF REPRESENTATIVES**

**Committee on Small Business  
Subcommittee on Regulatory Reform and Oversight**

**Data Protection and the Consumer:  
Who Loses When Your Data Takes a Hike?**

**Testimony of**

**Lisa J. Sotto, Esq.  
Partner  
Chair, Privacy and Information Management Practice  
Hunton & Williams LLP  
200 Park Avenue  
New York, NY 10166  
(212) 309-1223  
lsotto@hunton.com**

**May 23, 2006**

Good morning. My name is Lisa Sotto and I am a partner in the New York office of the law firm of Hunton & Williams LLP. I head the firm's Privacy and Information Management Practice and also serve as Vice Chairperson of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee. Thank you for the opportunity to participate in this hearing. I am doing so on my own behalf and my views should not be attributed to Hunton & Williams, any client of the firm, or the DHS Data Privacy and Integrity Advisory Committee.

This morning, I will address three topics: (1) state security breach notification laws, (2) information security requirements applicable to U.S. businesses, and (3) my recommendations for a federal security breach notification law.

## **1. State Security Breach Notification Laws**

In 2002, California enacted SB 1386, which became effective July 1, 2003. It is because of this law that we know about the many information security breaches that have occurred during the past several years. Essentially, the law requires organizations that own or license unencrypted, computerized personal information about California residents to notify those individuals if the security of their data was compromised.

Since the spate of publicized security breaches in 2005, 29 other states (in addition to California) have passed security breach notification laws. Similar legislation is pending in 11 other states.

While the various state breach notification laws are similar in many respects, they are not harmonized and contain some significant differences. For example, in 15 states, there is a harm threshold for notification. In Idaho, Kansas and New Jersey, an entity that suffers a data security breach is not required to notify individuals whose personal information may have been compromised if the entity determines that there has been no misuse of the information or that misuse is not reasonably likely to occur as a result of the breach. The trend in recently-enacted state breach laws is to include a harm threshold.

Another difference among state breach laws is in the definition of "personal information." Typically, "personal information" is defined in these laws as an individual's name *in combination with* Social Security Number; driver's license number or state ID card number; or account, credit or debit card number. Thus, if there is a security breach involving the unauthorized acquisition of "personal information" that could lead to identity theft, the entity that has suffered the breach must promptly notify affected individuals. In some states, however, the definition of "personal information" is broader. For example, in North Dakota, the definition includes date of birth and mother's maiden name, thus substantially broadening the notification requirement.

In addition, while most state breach laws cover only computerized data, North Carolina and Wisconsin also cover information maintained in hard copy format.

Some state breach laws contain additional notification requirements. For example, in Maine, New York, North Carolina and New Jersey, it is necessary to notify state agencies of a data breach. In numerous states, an affected entity also must notify consumer reporting agencies.

Needless to say, the variations in the 30 state security breach notification laws make compliance on a nationwide basis a complex matter.

## **2. Information Security Requirements Applicable to U.S. Businesses**

I will now briefly outline the information security requirements applicable to businesses in the United States. First, the Gramm-Leach-Bliley Act's ("GLB") Safeguards Rule requires that financial institutions develop, implement and maintain a comprehensive, written information security program that contains administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer data. These safeguards should be appropriate to the size and complexity of the entity, the nature and scope of the entity's activities, and the sensitivity of the customer information the entity maintains. Entities that are subject to the Safeguards Rule also must (i) designate an employee to coordinate the entity's information security program, (ii) identify reasonably foreseeable risks to the security of customer information, and (iii) require service providers by contract to implement and maintain similar safeguards. In addition, every covered entity must continually evaluate and adjust its information security program in light of ongoing testing and monitoring of the system.

Another law that requires a formal, comprehensive information security program is the Health Information Portability and Accountability Act of 1996, known as HIPAA. HIPAA's Security Rule applies to electronic protected health information. Like GLB, HIPAA adopts a flexible and scalable approach to information security. The Security Rule states that "[c]overed entities may use any security measures that allow the covered entity to reasonably and appropriately implement the [required security] standards." In deciding which security measures to use, the covered entity must take into account (i) its size, complexity and capabilities, (ii) its technical infrastructure, hardware and software security capabilities, (iii) the cost of various security measures, and (iv) the probability and criticality of potential risks to its electronic protected health information.

A third information security requirement applicable to many U.S. businesses is found in California AB 1950 and its analogs in other states, such as Arkansas and Texas. AB 1950 requires businesses that own or license personal information about California residents to implement and maintain reasonable security procedures to protect the information from unauthorized access, destruction, use, modification or disclosure. The law also requires businesses that disclose personal information to nonaffiliated third parties to require by contract that those third parties maintain reasonable security procedures.

Pursuant to the Fair and Accurate Credit Transactions Act, the Federal Trade Commission ("FTC") promulgated a rule in 2004 that requires businesses to take reasonable steps to guard against unauthorized access to or use of consumer report information in connection with its disposal. In short, the Disposal Rule requires businesses to take steps to securely dispose of consumer report information. Several states have even broader data disposition laws. These laws generally require that, when a company is ready to dispose of records containing personal information, the company must take reasonable steps to destroy the records so they become unreadable or undecipherable. States that have such records disposition laws in place include Arkansas, California, Georgia, Texas and Wisconsin.

In addition, other laws may create security obligations indirectly. For example, the FTC has applied Section 5 of the Federal Trade Commission Act to sanction what it believes to be inadequate security as an “unfair” trade practice.

### **3. Recommendations for a Federal Information Security Law**

Given the panoply of breach notification laws and information security requirements, I believe a federal law that would preempt similar state laws is critical. Because data often flows beyond state boundaries, a federal law would ensure that (i) personal information is subject to security requirements that are uniform throughout the nation and (ii) affected residents of every state would be notified of a data breach. Such a federal law should require businesses that collect and store sensitive consumer data to maintain reasonable security procedures to safeguard that data. This would provide consumers with uniform protection, regardless of where they live.

With respect to the breach notification requirements, I would advocate use of the California definition of “personal information” rather than an expanded definition adopted by some other states. The California definition is narrowly crafted to include only that information which is most commonly used by fraudsters to commit identity theft. Since the purpose of breach notification is to inform individuals of events that might cause them harm, there is no need to expand the definition to include data whose compromise would not subject an affected individual to identity theft or account fraud. In addition, I believe any federal law should contain a harm threshold. Notification should be required only if there is a real risk of harm resulting from a data breach. Finally, I would suggest that any federal law focus on computerized data rather than data maintained in another medium. Only information maintained in electronic format can be subject to the high volume of harm that these laws are specifically intended to combat.

I appreciate the opportunity to appear before you today to address these important issues. I would be glad to answer any questions you may have. Thank you.