Information Technology Industry Council

Written Testimony of
Yael Weinman

Vice President, Global Privacy Policy and General Counsel
Information Technology Industry Council (ITI)

Before the
Subcommittee on Consumer Protection,
Product Safety, Insurance, and Data Security

U.S. Senate Committee on Commerce, Science, and Transportation

Getting it Right on Data Breach
and Notification Legislation in the 114th Congress

February 5, 2015

Written Testimony of:
Yael Weinman
VP, Global Privacy Policy and General Counsel

Information Technology Industry Council (ITI)

Before the:
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security
U.S. Senate Committee on Commerce, Science, and Transportation

Getting it Right on Data Breach and Notification Legislation in the 114th Congress

February 5, 2015

Chairman Moran, Ranking Member Blumenthal, and Senators of the Subcommittee, thank you for the opportunity to testify today. My name is Yael Weinman and I am the Vice President for Global Privacy Policy and the General Counsel at the Information Technology Industry Council, also known as ITI. Prior to joining ITI, I spent more than 10 years as an attorney at the Federal Trade Commission, most recently as an Attorney Advisor to Commissioner Julie Brill.

ITI is the global voice of the technology sector. The 59 companies ITI represents—the majority of whom are based in the United States—are leaders and innovators in the information and communications technology (ICT) sector, including in hardware, software, and services. Our companies are at the forefront developing the technologies to protect our networks. When a data breach occurs, however, we want a streamlined process that helps guide how consumers are informed in cases when there is a significant risk of identity theft or financial harm resulting from the breach of personally identifiable information. In my testimony today, I will focus on several of the critical elements necessary to be considered by Congress in developing a federal legislative framework for data breach notification in the United States.

"Year of the Breach"

We have all heard 2014 referred to as "the year of the breach," but the reality is that data breaches did not just come on the scene last year—they surfaced quite some time ago. While companies and financial institutions spend tremendous resources to defend their infrastructures and protect their customers' information, it is an ongoing virtual arms race. Organizations race to

keep up with hackers while the criminals scheme to stay one step ahead. Unfortunately, it is no longer a matter of *if*, but a matter of *when*, a criminal hacker will target an organization. And when certain information about individuals is exposed, those consumers may be at a significant risk of identity theft or other financial harm. Year after year, identify theft is the number one category of fraud reported to the Federal Trade Commission.[1] I would expect that when the 2014 statistics are released, identity theft will continue to top the list.

51 Different Breach Notification Requirements

As a result of this troubling landscape, over the years, state legislatures across the country enacted data breach notification regimes. Currently, there are 51 such regimes—47 states and four U.S. territories.[2] Consumers across the country have received notifications pursuant to these laws. I have received more than one such notice myself, and I imagine some of you may have as well.

The current scope of legal obligations in the United States following a data breach is complex. Each of the 51 state and territory breach notification laws varies by some degree, and some directly conflict with one another. For example, Kansas requires that notification to consumers "must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system."[3] Connecticut's notification requirement to consumers is similar, but not identical. It requires notification to "be made without unreasonable delay, subject to [a law enforcement request for delay] and the completion of an investigation…to determine the nature and scope of

[1] See Federal Trade Commission, Consumer Sentinel Network Data Book for January – December 2013 (February 2014) available at http://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf; and Federal Trade Commission, Consumer Sentinel Network Data Book for January – December 2012 (February 2013) available at http://www.ftc.gov/sites/default/files/documents/reports/consumer-sentinel-network-data-book-january/sentinel-cy2012.pdf.

[2] The District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands each adopted a data breach notification law. New Mexico, South Dakota, and Alabama have not yet enacted breach notification laws.

[3] Kan. Stat. § 50-7a02(a).

the incident, to identify individuals affected, or to restore the reasonable integrity of the data system."[4] Florida, however, mandates a strict timeline and requires that notification be made to consumers no later than 30 days unless law enforcement requests a delay, regardless of the status of the forensic investigation into the scope of the breach.[5]

The complexities, however, are not limited to the timeline for notification. There are other significant variances among these state and territory laws, including what circumstances give rise to a notification requirement, how notifications should be effectuated, and what information should be included in notifications.

A Way Forward: A Single Uniform Data Breach Notification Standard

Federal data breach notification legislation offers the opportunity to develop a single uniform standard. ITI is currently updating a set of principles that we believe should be reflected in any federal data breach legislation you consider. I will be happy to share those with you upon their completion, which I expect to be very soon. Outlined below are several of these key policy recommendations.

Consumer Notification

Notifying individuals that their information has been compromised is an important step that then enables them to take protective measures. Notification to consumers, however, is not productive if all data breaches result in notifications. If that were the case, consumers would not be able to distinguish between notices and determine which ones warrant them to take action. Notification should be made to consumers if an organization has determined that there is a significant risk of identity theft or financial harm. Upon receipt of such a notice, consumers can then implement measures to help avoid being financially damaged.

[4] Conn. Gen Stat. § 36a-701b(b).

[5] Fla. Stat. § 501.171.

The process of determining whether there is a significant risk of identity theft or financial harm will include the examination of a number of factors, including the nature of the information exposed and whether it identifies an individual. Accordingly, efforts to define "sensitive personally identifiable information" in legislation should be carefully considered to ensure that over-notification does not ensue as a result of an overly broad definition that includes information, which, if exposed, does not in fact pose a threat of identity theft or financial harm. Determining whether there is a significant risk of identity theft or financial harm may also turn on factors such as whether the information exposed was unreadable. If data is unreadable, its exposure will not result in a risk of financial harm, and therefore notification would not be appropriate.

Consumers will be best served if they are notified not about every data breach, but about those that can cause real financial harm so that they can take precautionary actions only when they are in fact necessary. These actions can often involve expensive and inconvenient measures and should only be borne by consumers when there is a significant risk of identity theft or financial harm.

Timing of Notification

Mandating that companies notify consumers of a data breach within a prescribed timeframe is counterproductive. Recognizing the sophistication of today's hackers, and the challenging nature of the forensic investigation that ensues following the discovery of a breach, federal legislation must provide a realistic, flexible, and workable timeframe for consumer notification. Companies must be afforded sufficient time to remedy vulnerabilities, determine the scope and extent of any data breach, and cooperate with law enforcement. In certain instances, law enforcement agencies urge organizations to delay consumer notification so that suspected hackers are not alerted and driven off the grid. Sufficient flexibility in the timing of notification allows law enforcement to effectively pursue hackers, and ensures that consumers are neither notified with incomplete or inaccurate information nor notified unnecessarily.

Federal Preemption

A federal law that preempts the current patchwork of 51 different state laws would provide considerable benefits. A federal data breach notification requirement without federal preemption would accomplish nothing other than adding a 52nd law to this patchwork. Federal preemption ensures that consumers will receive consistent notifications, and thus they will be more easily understood. For organizations, it will streamline the notification process, enabling organizations to redirect resources currently being devoted to comply with 51 different notification laws. Such resources can be better utilized following a data breach, which requires a myriad of important steps, including investigating the breach, determining its scope, remedying vulnerabilities, and cooperating with law enforcement. One uniform framework allows organizations to make consistent determinations about who should be notified, when those individuals should be notified, and what information should be included in the notification.

No Private Right of Action

We urge you to avoid legislation that includes a private right of action for violations of a data breach notification regime. The best way to protect consumers is not to empower the plaintiff's bar to pursue actions that are ultimately only tangential to consumer injury. Appropriate government enforcement for violations of data breach notification legislation is the proper remedy.

2015: The Year of Federal Data Breach Notification Legislation

A federal data breach notification law that preempts the current regime would be an important step forward for 2015—the year after the "year of the breach." At ITI, we hope that 2015 is the "year of a federal data breach notification law." Thank you again for the opportunity to share our thoughts on a federal data breach notification regime, and I am happy to answer any questions you may have.