

**Opening Statement of the Honorable Lee Terry**  
**Subcommittee on Commerce, Manufacturing, and Trade**  
**Hearing on “Reporting Data Breaches: Is Federal Legislation Needed to Protect**  
**Consumers?”**  
**July 18, 2013**

*(As Prepared for Delivery)*

In today’s economy nearly everyone leaves a digital footprint. Even if you made a concerted effort to avoid smart phones, laptops, and social media, you would have a difficult time keeping your personal information from being held in an electronic database somewhere.

Consumers should have the peace of mind that their data is protected in a responsible way. But with all types of nefarious activities online, so-called “hacktivists” are finding new ways to steal data. So in the event that our personal data becomes exposed, we need to be able to trust that the companies in possession of our data will notify us of the exposure. And certainly it is in those companies’ best interest to notify promptly and clearly in order to preserve a trusting relationship with consumers.

Given these considerations, the question before us is: What are the rules of the road for companies that experience a breach in their data stores?

Currently, the laws that govern data breach notification are a patchwork of state and territory-specific statutes. Unfortunately, they tend to differ from each other in many ways. For example, while a number of states have adopted a common definition of “personal information,” even more states have adopted alterations to that definition, and those vary unpredictably. This definition is important because it triggers the duty to notify of a breach.

Three states include encrypted or redacted data in the definition of “personal information,” whereas the rest do not. Five states include public records in the definition. Meanwhile, four states protect an individual’s date of birth and mother’s maiden name as “personal information.”

With at least 48 of these various state and territory-specific laws on the books, you can see how the cost of compliance could add up. The global price tag of cyber crime has been calculated at around \$110 billion annually, and we should not add unnecessary compliance costs to this. Adding to the confusion, these laws also tend to vary on the number of days that can elapse after a breach before notification as well as the method of notification.

Even small breaches can cause a compliance headache. In one recent example, a large company experienced a breach where the personal information of just over 500 consumers was compromised. In comparison to other recent breaches involving tens of millions of consumers this may seem small. Yet it turns out that these 500 consumers lived in 44 different states and therefore had to be notified pursuant to 44 different sets of rules.

We must remember that where a breach in data is intentional; for example, if it is done by a “hactivist”—the company holding the data is also a victim. Burdening these entities with overly complicated notification rules is not a solution to the harms that result from the exposure of personal information.

And with that, I look forward to hearing the testimonies of our witnesses and to learning about whether we can improve the current legal landscape for breach notification.

###