

**Responses to Additional Questions for the Record submitted by The Honorable
Michael C. Burgess**

Elizabeth Hyman

Executive Vice President, Public Advocacy

TechAmerica, the public policy department of CompTIA

March 18, 2015

1. The President recently called for a single, national standard for breach notification legislation. Do you have a response to the language he proposed? Please discuss.

We appreciate the President's endorsement of a national breach notification standard, but we have some concerns about the specifics of his proposal, such as:

- 1) The definition of "Sensitive Personally Identifiable Information" should contain an exception for information accessible through public records;
- 2) The 30 day timeframe for notification may not be long enough for companies to conduct a thorough risk assessment;
- 3) The 30 day timeframe is similarly unrealistic for receiving an exemption if a risk assessment finds that there was no reasonable risk of harm from the breach;
- 4) It does not contain a provision allowing substitute notification should the breached entity not have necessary contact information;
- 5) It does not ban private rights of action.

We simply cannot support a data breach notification bill that contains, from our perspective, such significant shortcomings.

2. Given the activity of States regulating data security in the last few years, is there a benefit for industry if Congress sets a national standard for reasonable data security. Would you support a preemptive reasonable data security standard? Please explain.

There is absolutely a benefit for industry if Congress sets a national standard for data security, as long as that standard is reasonable. However, we do not believe that data security requirements should be specifically enumerated by legislation, and should instead be determined by the FTC with assistance from industry to determine a set of "best practices." While our testimony focused specifically on data breach notification, and not data security, we have similar concerns about companies', particularly SMBs, ability to comply with a complex web of conflicting state data security requirements. A national standard would protect consumers by putting data security requirements in place for the states that currently do not have them, and benefit the tech industry by providing a clear standard by which all companies must abide.

3. Would your members support data security and breach notification legislation that does not contain preemption of State law?

Quite simply, we would not support legislation that does not preempt State law. The primary reason we have advocated for a national standard is to alleviate the compliance burden for companies who have to comply with the 47 different state standards. If a federal standard does not preempt the state standard, it will not accomplish that goal and will instead merely function as a 48th standard atop which states can add their own requirements. Compliance would remain as difficult as it is in today's environment.

4. How do you define preemption that would effectively eliminate the existing patchwork of State laws?

We have never advocated for a specific definition of preemption, but have long-supported strong preemption language that would ensure that the federal standard is the only standard with which companies must comply for notifying consumers following a breach. As stated earlier, it must be made clear that states cannot add additional breach notification requirements atop the federal standard.

5. How do you believe state common law should be treated in federal data security and breach notification legislation? Should it be preempted?

Federal data security and breach notification legislation should preempt state common law to the extent that individuals cannot sue companies simply for failing to comply with the federal security and breach notification standards. However, federal legislation should not preempt state common law that falls outside the scope of the legislation. Protection of consumer data must be a priority for companies, and we must not strip away consumers' ability to protect themselves.

6. Please explain the issues that could develop in the marketplace if a federal data security and breach notification bill does not preempt State law.

As explained earlier, a bill that does not preempt State law will simply add more confusion to the marketplace than we already have today. It will add one more law to the massive list of State laws that companies must already comply with. Ultimately, it would serve very little purpose.

7. Do you support allowing State Attorneys General to enforce a federal data security and breach notification law if the law preempts current State law? Are there other factors that should be considered in extending this enforcement authority?

We absolutely support allowing State Attorneys General to enforce a federal law. Doing so would put more cops on the beat to help protect consumers. However, the law must ensure that companies cannot be punished at both the state and federal levels for the same violation of the statute.

8. There was testimony during the hearing that companies undertake investigations after a breach is discovered. Please explain the steps of a data breach investigation and what information companies learn during this process.

Once a company suspects a breach, the first step is likely to determine the source of the breach and if it's too late to prevent information from being accessed. A company must then attempt to determine what was accessed, when it was accessed, how it was accessed, who it was accessed by, what they might do with the information, and what can be done to prevent a breach from happening again. Then it must ensure that its system integrity has been restored. Often these steps involve bringing in outside consultants and/or law enforcement for assistance, and can be expensive and time-consuming. The last thing companies should have to worry about at this critical point in time is which particular state laws apply to this particular breach and how to comply with each and every one of them properly.

9. The dangers of over notification for consumers in the long term have been outlined by States, companies and the Federal Trade Commission. Taking this into consideration, what should the risk trigger be for a company to notify individuals after a breach?

We have long advocated that any federal framework should require notification only when there is a risk that harm has or is likely to occur. Requiring notification without some threshold of harm risks overnotification of consumers.

10. If there is a deadline for notification following a breach, should the clock start after the breached entity has been able to secure and restore the breached system? How do the states approach this in their breach notification statutes.

We have long advocated that statutes should not contain a specific timeframe for notification and should instead require notification "without unreasonable delay" or within a "reasonable" time. All breaches are different, and creating a single timeframe for all breaches could prove problematic in certain situations. However, if a specific timeframe must be enumerated, we would suggest that the clock start after the entity has been able to conduct a risk assessment and secure their breached system. The risk assessment could take anywhere from days to months, depending on the breach, and notification before the assessment is concluded could prove damaging to the breached entity.

Most states do not require a specific timeframe for notification, and instead require notification "without unreasonable delay" and/or "in the most expedient time possible," and acknowledge that it may take time for companies to determine the scope of the breach and restore their systems. When states have laid out a specific timeframe, we have found that most states require notification within forty-five days following the discovery of the breach.

11. What are cyber attackers typically looking for when they attempt to breach your members' networks? Do you know if the purpose is typically to embarrass the consumer or to steal his or her information for financial gain?

We reached out to a number of members for feedback on this question and didn't receive the same answer twice, so it seems as if there is not one clear purpose for cyber attacks. Embarrassment appeared to be less of an incentive than financial gain, but we heard everything from "just poking around" to attempting to take down a company, to identity theft, to gaining access to a company's infrastructure for other nefarious purposes. Cyber attackers have many different reasons for carrying out attacks, and any legislation should acknowledge this fact.