

Subcommittee on Commerce, Manufacturing, and Trade
What are the Elements of Sound Data Breach Legislation?

Response of:

Ms. Jennifer Glasgow
Global Privacy and Public Policy Executive
Acxiom Corporation

Additional Questions for the Record

The Honorable Michael C. Burgess

- 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.**

Answer: We appreciate the Administration's focus on a single national standard for breach notification legislation. Acxiom does not believe that a new legislative proposal was necessary, since Congress has had the right basic provisions of a data breach notification bill under consideration for a number of years. However, we believe it is helpful for the Administration to weigh in supporting congressional action, as that may help build momentum for Congress's bill.

We do not believe that a 30-day notification requirement is in the public interest, and will discuss that in greater detail below.

- 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.**

Answer: Acxiom would support a uniform federal data security standard. There is far more variance in State data security obligations than in breach notification obligations. A uniform federal standard likely would provide greater protection for individuals by instituting a standard of protection that is higher than may be the case in some organizations today. Furthermore, conflicting State data security obligations are more problematic than conflicting breach notification obligations. Companies don't develop security systems for each state. They develop them for the entire U.S. and often for the entire world.

A federal standard needs to be clear. Vague standards can facilitate unwarranted litigation. The standard also needs to be flexible enough to adapt as threats and capabilities adapt. We are comfortable providing the FTC with authority, which addresses the issue of flexibility. However, the FTC standard needs to be sufficiently concrete that companies do not have to worry about finding themselves on the wrong side of a regulator's expectations without fair notice.

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

Answer: My testimony included the following suggested formulation:

No law, rule, regulation, requirement, standard, or other provision having the force and effect of law relating to data security or notification following a breach of data security may be imposed under State law or the law of a political subdivision of a State on a person subject to this Act.

Subcommittee on Commerce, Manufacturing, and Trade
What are the Elements of Sound Data Breach Legislation?

Response of:

Ms. Jennifer Glasgow
Global Privacy and Public Policy Executive
Acxiom Corporation

Other formulations also could be effective. Consumers need notice that is clear and meaningful; businesses need notice rules that are not unnecessarily inefficient and burdensome. Those two aims are both served by a single preemptive federal standard.

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

Answer: Liability provides a disincentive to practices that cause harm, and compensation to those who are harmed. The regulation provided by the bill will make unlawful breach notification practices that could cause harm. As for compensating injured parties, injuries typically do not arise from notification or lack of notification, but from the breach itself. For these reasons, we believe Congress very reasonably could conclude that State common law with respect to breach notification should be preempted. Companies are better served if there is uniformity and predictability in the law. State common law provides neither.

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

Answer: Congress would in essence be creating a 51st applicable law, which would only exacerbate the current problem. We would be better off without a federal law if it doesn't have preemption to establish a single standard. Congress would be making matters worse. If a federal law sits alongside a conflicting State law that is not preempted, consumers could receive more than one notice, which would be harmful by creating confusion. It would also be harmful because the added cost – again, in providing no benefit – ultimately will be borne by consumers and the economy.

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

Answer: While we prefer that federal law be enforced by federal entities, we also think it is important for sufficient resources to be available for enforcement. If the law is fully preemptive, we would not object to allowing State AGs to enforce the bill's requirements.

7. 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.

Answer: Breaches can come from many places - hackers trying to break in to someone's system, other companies or countries stealing confidential data for commercial gain, and insiders leaking data intentionally or unintentionally. Furthermore, breaches can be discovered by the breached company themselves via their own detection systems, discovered by law enforcement in the investigation of

Subcommittee on Commerce, Manufacturing, and Trade
What are the Elements of Sound Data Breach Legislation?

Response of:

Ms. Jennifer Glasgow
Global Privacy and Public Policy Executive
Acxiom Corporation

other unlawful conduct that may include the criminals' use of the stolen data, or discovered by investigative journalists. Also, a breach can be limited to one system or it can be distributed across many systems that may involve systems run by other entities or supported by vendors. Furthermore, it may take time to get subpoenas to investigate other parties, and law enforcement may need time to confiscate evidence before a breach becomes public and before the information is destroyed. Each of these factors can require a very different investigative, corrective, and restorative approach. Furthermore, investigations are not linear: you don't simply learn all at once about the problem and then fix it. A breached company may initially think the breach involved one system or one individual and investigate logs or other tracking records to determine the scope of the breach. Many times, this points to other systems, other individuals or other entities that also need to be investigated. Think of the process as iterative, often looping back on itself to necessitate more investigation after some fact is known.

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

Answer: It should be a reasonable risk of harm trigger. This is consistent with most of the existing state laws and the Gramm-Leach-Bliley Act. Furthermore, there is very little functional difference between terms such as "reasonable" or "significant" risk of harm, as we believe companies essentially would look at the facts in the same way when determining whether to notify.

- 9. Is it practical to toll a notification deadline in federal data security and breach notification legislation to allow the breached entity time to secure and restore the breached system? Do any States take this approach in their breach notification statutes? I don't know State requirements, but I assume many do provide for such temporary suspension. If you don't toll, you risk notifying before you've fully learned what happened.**

Answer: It is not practical to have a firm deadline for breach notification. "As quickly as reasonably possible" is the idea; Congress needs to determine how to shape that into a legal standard. As outlined in my answer to question 7, the timeframe for discovering, securing and restoring a breached system is not predictable. If there is a notification deadline, some breaches will notify before all the facts are gathered and may have to do additional notifications once the investigation has further developed. If facts are discovered after an initial notice, it could result in the confusion of an additional notice to the same consumers. Most breaches are discovered months after they take place, or have been going on for months. We should not force an artificial deadline, but instead allow the investigation and restoration to proceed to completion.

Subcommittee on Commerce, Manufacturing, and Trade
What are the Elements of Sound Data Breach Legislation?

Response of:

Ms. Jennifer Glasgow
Global Privacy and Public Policy Executive
Acxiom Corporation

- 10. 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?**

Answer: From our experience and based on breaches reported in the press, the cyber attackers are typically looking for data for financial gain, either from ID theft or other scams that require knowledge of certain personal information in order to conduct the scam. Even in the scam situations the objective is financial gain.

The Honorable Bobby Rush

- 1. It is my understanding that there are at least three categories of information that firms, such as Acxiom, provide information for. You discussed how consumers are able to correct errant information or opt out of marketing altogether. Are the changes consumers make to the marketing section carried throughout the other categories?**

Answer: Acxiom has three categories of information that we bring to the market. One is information for marketing purposes, another is information for risk mitigation and the third is telephone data for directory purposes. Each category is developed with the data specifically needed for that purpose and access, correction and opt-out rights appropriate for each. For marketing purposes, consumers can access, correct, delete elements or opt-out of all marketing uses via our website www.aboutthedata.com. We offer a complementary offline service for accessing and correcting the risk mitigation information because we do stronger authentication for this data that contains sensitive elements like SSN and DL#. For risk information we do not offer opt-out because we don't allow the bad buys to opt-out of the very systems designed to catch them. The final category, directories, contains names and phone numbers and is only compiled from public records and directory assistance. Consumers can opt-out of this, but we do not provide a correction feature.