Woodrow Hartzog
Associate Professor
Samford University's Cumberland School of Law
3-13-15

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.

   The version of the President's proposed language that I have seen has some commendable elements. It allows for a flexible definition of SPII to be modified by rulemaking, covers non-profit organizations, requires notice without unreasonable delay with a 30 day cap, empowers the FTC and provides a safe harbor when there is no reasonable risk of harm instead of a harm trigger. However, it is too preemptive of federal and state protections, improperly excludes paper records and other non-digital data, and has thin notice requirements, including no requirement to inform third parties like credit reporting databases under some circumstances and no requirement to list when the breach occurred. Sound data breach legislation should also include a nationwide requirement for businesses to provide reasonable data security.

2. In many cases, a breach in data security is the result of criminal hacking. Do you support private causes of action for data breaches against the companies that were victims of a breach? Please explain your position on private causes of action taking into consideration the fact that private causes of action expose a company to liability when the real culprit is the intruder/criminal that hacked the company's system.

   I support private causes of action in instances where demonstrable harm resulted from unreasonable data security practices. Not every data breach should give rise to liability. However, consumers can suffer harm as a result of negligent data security practices, which is precisely what private causes of action are intended to remedy. Companies are victims of the hackers, but also sometimes culpable for failing to protect data entrusted to them by consumers.

The Honorable Tony Cárdenas

1. Recently, I had an amendment included in the National Defense Authorization Act (NDAA) to help smaller defense subcontractors who may not have information technology departments prepare themselves for cyber-attacks. What aspects of data breach legislation take into account the differences between big and small businesses?

   A data security requirement using a reasonableness standard would presumably incorporate the differences between big and small businesses. A small business collecting only small amounts of personal information does not need to have the exact same data security as large corporations like Target and Microsoft. The FTC has said as much in its statement issued with its 50th data security settlement, saying, "a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it

holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."

2. As the recent data breach attacks on Sony show, cybersecurity issues can quickly lead to the release of private and intimate information of many Americans and drastically harm a company's financial well-being. With even the largest of American companies at risk, what financial risks do we continue to run by not putting together a bipartisan solution that can be signed by the President?

   There are few issues more important to commerce and our national infrastructure than data security. While the FTC has admirably regulated data security for the past twenty years, it could benefit from more resources and specific rulemaking authority. Poor data security regulation not only runs the risk of financial loss from fraud, it also risks financial loss in the form of lost consumer confidence. People will be forced to withdraw from the marketplace if they cannot trust that their information will be protected.

   However, it is important to emphasize that federal data breach legislation could do more harm than good if it weakens the existing hard-won state and federal protections. Companies already have obligations to keep data secure and notify users in case of a breach. These obligations are not dramatically different from each other and virtually all data security laws simply require a reasonable adherence to industry standards. While federal data breach legislation could provide more protection, there is no urgency to produce a weaker solution.

3. Have consumers, whose buying habits, identities, and financial information are at risk, been notified of how much of their information is currently at risk?

   In a technical sense, consumers are notified when their data is breached and they are reminded daily by the media of how vulnerable companies are. But in practice, this only somewhat benefits consumers. Data security is opaque to consumers. Short of eternal vigilance, credit freezes and withdrawals from the marketplace, consumers are limited in the ways they can minimize the risk of personal disclosure in the modern age. This is why any federal solution should include data security requirements and breach notice requirements to third parties such as state attorneys general, credit reporting agencies, and the media.