Hope Emerges at Senate Data Security Hearing – But Will Congress Grab the Brass Ring?

Laura Riposo VanDruff

October 10, 2021

On October 6, 2021, the Senate Commerce Committee conducted its second in a series of hearings dedicated to consumer privacy and data, this time addressing Data Security. Similar to last week's privacy hearing, the witnesses and Senators appeared to agree that federal data security standards – whether as part of privacy legislation or on their own – are urgently needed. If there were to be consensus around legislative principles, the hearing provides clues about what a compromise might look like.

Prepared Statements. In their opening statements, the witnesses emphasized the need for minimum standards governing data security.

- James E. Lee, Chief Operating Officer of the Identity Theft Resource Center, explained that without minimum requirements, companies lack sufficient incentives to strengthen their data security practices to protect consumer data. Lee also advocated for more aggressive federal enforcement rather than the patchwork of state actions, which, he said, produce disparate impacts for the same conduct.

- Jessica Rich, former Director of the FTC's Bureau of Consumer Protection and counsel at Kelley Drye, emphasized that current laws do not establish clear standards for data security and accountability. She advocated for a process-based approach to prevent the law from being outpaced by evolving technologies and to ensure that it accommodates the wide range of business models and data practices across the economy. Among her recommendations, Rich suggested that Congress provide the FTC with jurisdiction over nonprofits and common carriers and authority to seek penalties for first-time violations.

- Edward W. Felten, former Deputy U.S. Chief Technology Officer, former Chief Technologist of the FTC's Bureau of Consumer Protection, and current Professor of Computer Science and Public Affairs at Princeton University, focused on the need to strengthen the FTC's technological capabilities, including increasing the budget to hire more technologists. Notably, Felten advocated for more prescriptive requirements in data security legislation such as requiring companies to store and transmit sensitive consumer data in encrypted form and prohibiting companies from knowingly shipping devices with serious security vulnerabilities.

- Kate Tummarello, Executive Director at Engine, a non-profit organization representing startups, addressed the importance of data security for most startups. Tummarello advocated for FTC standards or guidance with flexible options. Cautioning against overburdening startups, Tummarello explained that newer companies take data security seriously because they do not have the name recognition or relationships with consumers that larger companies may have,

and a single breach could be extremely disruptive. Additionally, Tummarello highlighted that the patchwork of state laws provides inconsistent and unclear data security guidance and imposes high compliance costs.

Discussing a Federal Data Security Bill

- Preemption. Witnesses agreed that a preemptive federal law does not necessarily mean a weaker law. Rich offered a middle ground, supporting preemption, but stating the law should fully empower the state AGs to enforce it.
- Private Right of Action. Tummarello expressed concern that lawsuits across the country would contribute to the "patchwork" of laws that increase compliance costs. However, if a private right of action were necessary, she would support only a narrow private right of action with sufficient notice and guardrails, particularly to protect startups vulnerable to bad faith litigation. Lee demurred on whether a private right of action was needed but emphasized that consumers need to be protected no matter what state they live in. Rich stated that if the legislation is strong enough – with robust protections and remedies, full enforcement authority for the states, and significant resources for the FTC – it will protect consumers without the need for a private right of action. However, Rich also described "middle grounds" that could bridge the divide.
- Sensitive Data. Although there were some questions about what constitutes sensitive data, the witnesses agreed that both biometric data and data about children should have heightened protections. Felten addressed concerns regarding artificial intelligence and facial recognition. Lee discussed the importance of protecting biometric data because it is permanent and cannot be changed – unlike a credit card number – if it is compromised.
- Process-Based Approach. Rich emphasized the need for a "scalable" federal law that takes a process-based approach so that it does not quickly become obsolete. She added that the FTC could issue more detailed guidance on a regular basis to highlight particular technologies and safeguards that companies should consider. In contrast, Felten supported specific safeguards that the FTC would require through rulemaking, and Tummarello supported an FTC rule or guidance that would give companies a "menu" of safeguards to consider.
- Inclusion with Data Privacy Bill. All witnesses supported including data security provisions into a federal privacy bill, but Rich stated that a data security law could prevent considerable consumer harm as a stand-alone measure.

FTC's Role and Enforcement.

- FTC as Enforcer. Similar to last week's hearing, all witnesses agreed that the FTC was the agency best equipped to oversee and enforce a federal data security law.
- Resources Needed. Felten noted that the FTC only has about ten technologists on staff, but could use 50-60 people in technologist roles to supplement its enforcement efforts. Rich added that technologists need a career path at the FTC, and that the FTC should reexamine the complicated ethics rules governing what technologists may do after they leave the FTC's employment.
- First time penalties. All witnesses agreed that the FTC should be able to seek penalties for first-time violations. Tummarello, however, said that she supports first-time penalties only if there are clear rules of the road.

Overall, the hearing made clear that there are more areas of agreement than disagreement. The key questions are: (1) Can Congress resolve differences related to a private right of action, whether by ensuring strong protections without it or by compromising on a narrow private right of action? (2) Will Congress be willing to pass federal data security legislation on its own? We will continue to monitor developments on this issue and provide updates as they occur.