Akin®

Energy & Commerce Subcommittee Holds Hearing on Data Security and Breach Notification; FTC Releases "Internet of Things" Report

Jan 27, 2015

Reading Time : **3 min**

By: Francine E. Friedman, Anthony T. Pierce, Natasha G. Kohne, Mathew C. Thomas (Senior Public Policy Specialist)

On the Democratic side, Ranking Member Janice Schakowsky (D-IL) also called for a single federal standard for breach notification and data security, but cautioned that any legislation should not weaken current state protections. She also said that state attorneys general should retain the power to enforce state consumer protection laws that may apply in the event of a breach. Full committee Ranking Member Frank Pallone (D-NJ) echoed her sentiments and stated that he would not support any bill that is weaker than the strongest state law in place.

The overarching theme of the hearing was whether federal standards for data security and breach notification should preempt existing state laws. Almost all committee members present indicated that they would support strong federal preemption, with Democrats adding small caveats that any federal standard should not weaken existing state protections. Among the witnesses, three-fourths supported federal preemption when coupled with a risk-based trigger for notification, while the fourth (Mr. Woodrow Hartzog, an associate professor at Cumberland School of Law) argued against preemption if it would weaken state protections; prohibit state enforcement, as well as federal enforcement; and be tied to a risk-based trigger for notification.

Among the first three witnesses, recommendations to the committee were generally the same:

- Enact a federal data security and breach notification standard that preempts the existing patchwork of state laws.
- Notification should be required only when personally identifiable information (PII) is actually accessed or acquired, and there is a reasonable potential for harm.
- If Personally Identifiable Information (PII) is encrypted or otherwise rendered unusable, no notification should be required.
- There should be a comprehensive definition of what constitutes PII.
- Legislation should be flexible and technology-neutral.
- There should be no private right of action against any company for compliance with data security and breach notification standards.
- There should be a reasonable, flexible deadline for breach notification.
- Civil penalties should be reasonable, tied to actual harm and capped.

Mr. Hartzog cautioned the subcommittee against preempting state laws, arguing that doing so could weaken protections already in place and could create gaps in protection for certain types of information. He instead argued for the status quo of state regulation, along with additional rulemaking authority for the Federal Trade Commission (FTC) to develop stricter data security requirements. While opposed to federal preemption, he did state that, if Congress does decide to preempt state laws, it should be minimal and should not be tied to a harm-based trigger for notification.

Separately, the FTC released a staff report today entitled "The Internet of Things: Privacy & Security in a Connected World." The report follows a workshop the FTC held on November 19, 2013, to address growing privacy and security concerns with respect to the increasing use of devices connected to the Internet, and outlines the benefits and risks of the Internet of Things (IoT) and the comments received at and following the workshop, as well as FTC recommendations for the ideas and concerns expressed. The FTC vote to issue the staff report was 4-1, with Commissioner Wright voting no. In his dissent, Wright said that the FTC should not have released the report, because its recommendations are based on a single workshop.

The FTC, and participants in the workshop, identified a number of benefits and risks that the IoT poses. Examples of benefits include "smart health" technology (allowing patients and medical practitioners to gather data and communicate more effectively), smart metering and smart appliances that help to control home energy use, home automation systems, and

connected vehicles. Despite these many and varied benefits, the Commission separates risks into two key areas: 1) security risks and 2) privacy risks.

During the workshop, participants also discussed how the longstanding Fair Information Practice Principles (FIPPs) of notice, choice, access, accuracy, data minimization (limiting the amount of data collected), security, and accountability should apply to the IoT space. The Commission states that discussion centered on four FIPPs in particular: data security, data minimization, notice, and choice. While participants were agreed on the need for manufacturers of IoT devices to incorporate reasonable security measures, they were more divided on the applicability of data minimization, notice, and choice. On minimization, participants expressed concern that limiting data collection could hamper innovation and the potential benefits of the IoT. On notice and choice, some participants expressed concern about the feasibility of giving consumers notice of and the option to control what data is collected. Another concern was the lack of graphic interfaces on many IoT devices, which makes delivering notice through the device difficult.

Recommendations by the Commission include encouraging manufacturers of IoT devices to incorporate security by design practices, train employees in proper security practices, minimizing data collection and de-identifying data collected, and provide consumers with multiple ways to learn about and control the ways data may be collected.

With respect to the need for federal legislation, the Commission declined to call for legislation to regulate the IoT, but again reiterated its position that data security, breach notification, and privacy standard legislation is necessary.

Categories

Policy & Regulation | Cybersecurity, Privacy & Data Protection