Akin®

State Lawmakers Go After IoT Security Risks

Nov 15, 2019

Reading Time : **4 min**

By: Virginia Hiner Antypas, Jennifer L. Richter

While connected devices offer unprecedented advancements in terms of efficiency and convenience, the continued proliferation of these devices has raised concerns about the risk of hacking and unauthorized access. As a result, state and federal lawmakers have begun to take action to regulate IoT device security. For example, California and Oregon have already passed laws that will require manufacturers to incorporate mandatory minimum security features in IoT devices beginning Jan. 1, 2020. Similar measures have been introduced in a number of other states.

Federal legislators also are paying attention to this issue, and have introduced a number of IoT bills that are pending in the House and Senate. Since regulation of these devices is on the rise, it is imperative that IoT device manufacturers begin considering the risks associated with their products and take measures to ensure that consumer data remains secure.

State Efforts to Regulate IoT Device Security

California is the first state to have enacted legislation regulating the security of IoT devices. Starting in 2020, connected devices that are manufactured, sold or offered for sale in California must be equipped with "reasonable security" features. Under California law, the onus to ensure that a connected device is "reasonably secured" rests with the manufacturer. What constitutes "reasonable security" under California law is not precisely defined, because whether a feature is reasonable will necessarily depend upon the nature and use case for the specific device (e.g., a security feature that is reasonable for a connected coffee pot may not be reasonable for a connected health device).

In light of this, California provides three broad parameters to evaluate the reasonableness of a particular security feature. To be deemed reasonable, a security feature must be:

1. Appropriate to the nature and function of the device;
2. Appropriate to the information it may collect, contain, or transmit;
3. Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification or disclosure.

The statute does not prescribe a safe harbor for compliance. Whether a security feature is reasonable will likely be determined over time through enforcement actions.

Following California's lead, Oregon adopted a law requiring manufacturers of connected devices sold within the state to adopt "reasonable security features" that are appropriate to the nature and function of the particular device and the type of information it collects or transmits. While the Oregon statute largely tracks the new California law, there are a few key differences. Most notably, any devices or "other physical objects" capable of connecting directly or indirectly to the Internet and that are assigned either an Internet Protocol or Bluetooth address are covered under California's statute, whereas Oregon's law is more limited, applying only to devices that are "used primarily for personal, family, or household purposes." In addition, only the Oregon law provides for a private right of action.

A number of states have considered legislation similar to the California and Oregon IoT laws, including Illinois, Kentucky, Massachusetts, Maryland, New York, Rhode Island, Vermont and Virginia. To date, none of the proposed bills were enacted and, with the exception of Massachusetts, all of the aforementioned state legislative sessions have adjourned. The proposals considered in 2019 have generally followed California's model, requiring manufacturers to build "reasonable" security features into their connected devices, with some variations.

For example, a bill proposed in Virginia contained several additional requirements, including a requirement that manufacturers demonstrate their conformity with industry standards for cybersecurity and resiliency, and a requirement that manufacturers notify the state's chief information officer upon becoming aware of device vulnerabilities that put more than 500 users at risk. In addition, some states have considered separate legislation focused specifically on voice-activated "smart speaker devices." Although none of these proposed state bills were successful during the 2019 legislative session, lawmakers' growing interest in these issues

indicates that we will likely see more IoT-related legislation introduced, and possibly enacted, in 2020.

Federal Legislation

Congress has not yet passed federal legislation governing the security of IoT devices, but federal lawmakers have been increasingly focused on the issue. Over the past year, a number of measures were introduced into both the House and Senate. For example, on Oct. 22, a group of Democratic representatives introduced the Cyber Shield Act in the House. If enacted, the Cyber Shield Act would direct the Commerce Department to establish an advisory committee of cyber experts from government, industry and academia to establish "cyber benchmarks" for IoT devices. Device makers could voluntarily certify that products meet the cyber benchmarks by placing a "Cyber Shield" label on conforming products.

Federal lawmakers also are considering several bills that would grant the Federal Trade Commission (FTC) broader authority to regulate IoT devices, including the Protecting Privacy in Our Homes Act, which was introduced by Sen. Cory Gardner, R-Colo., on Sept. 24, 2019. This proposed bill would direct the FTC to adopt new rules requiring manufacturers of IoT devices that contain microphones or cameras to provide notice "on the packaging" that the device contains such components.

Similarly, Rep. Seth Moulton, D-Mass., recently introduced in the House the Automatic Listening Exploitation Act, which would grant the FTC and state attorneys general enforcement authority over manufacturers of smart speakers and doorbells that record users' private conversations when the user has not activated the device. The bill would authorize penalties of up to $40,000 per violation and would also create data subject rights allowing consumers to have their recordings, transcripts and videos deleted.

Conclusion

The passage of IoT device security legislation in California and Oregon signals the start of a specific legal framework governing IoT. In view of the growing concern over IoT device security at both the state and federal level, more legislation is likely to follow, with the potential for stricter minimum security standards in the future. Penalties for non-compliance could be significant, particularly if lawmakers opt to provide for a private right of action or impose minimum statutory damages per violation, which could give rise to costly class-action lawsuits.

Manufacturers should take action to understand the requirements in California and Oregon in advance of the upcoming Jan. 1, 2020, implementation date, and continue to pay close attention to developing IoT laws and initiatives in the coming year.

Categories

Cybersecurity & Information Security

Federal Privacy Policy

State Privacy Policy