Not in My House – California to Regulate IoT Device Security

S. Wilson Quick
October 5, 2018

On Friday, Sept. 28, 2018, California Governor Jerry Brown signed into law first-in-the-nation legislation requiring that manufacturers include "reasonable security features" on any device that is "capable of connecting to the Internet"—commonly known as an "Internet of Things" (IoT) device. California Assembly Bill 1906 and Senate Bill 327, which contain identical text, won't go into effect until Jan. 1, 2020, but most manufacturers of IoT devices are going to need that lead time (if not more) to ensure the devices they put out into the market are compliant with the new law.

What Sort of Devices Are Affected?

The new law applies to any device with internet capability and its own Internet Protocol (IP) or Bluetooth address. This means that all sorts of devices—gaming systems, children's toys, smart door locks, Wifi-enabled fish tanks, and more—might be affected. If a product sold for the home (or office or car) of a California resident has internet capability, then it should be designed in compliance with the new law.

However, software that is sold separately from a device is exempt from the new law. These types of products typically are "add-ons" or "apps" that a consumer can download to an IoT device after purchase.

There are also additional exclusions for IoT devices that are otherwise regulated by federal law and for most devices designed for the healthcare industry.

Who Is Affected?

As written, the new law only applies to "manufacturers" of physical devices that are sold or offered for sale in California, or businesses that contract with a manufacturer to produce a device that will be sold in California.

Notably, the law does not apply to companies that purchase a "white-label" product for rebranding and sales only. However, any company whose business model relies on this type of arrangement should review its agreements with the original manufacturer to ensure that there is no question about who was responsible for the design and manufacture of the product.

What Does "Reasonable Security Features" Mean?

The new law is relatively vague about which types of security features will be considered "reasonable" by regulators. The onus is placed on individual manufacturers to determine what is reasonable, with the "nature and function" of the IoT device and the type of information being collected or transmitted as determining factors. Any built-in security feature should be designed to protect the device and the information stored within it from unauthorized access, destruction, use, modification or disclosure.

The law does provide some guidance relative to IoT devices that can be accessed via "authentication outside of a local area network." For those types of devices, the authentication system must either come with a preprogrammed password that is unique to each manufactured device (meaning no "default" password for each device off the assembly line) or contain a security feature that requires the consumer to create a new means of authentication the first time it is accessed. While helpful, both of these requirements leave some questions unanswered. For example, will regulators expect that preprogrammed passwords meet a certain standard of robustness?

Who Can Enforce the Law?

One positive of the new law for manufacturers is that it does not allow for a private right of action. Instead, only the California Attorney General and local city, county and district attorneys have "exclusive" enforcement authority. It remains to be seen what, if any, guidance the Attorney General's Office, as the only statewide regulator, will provide to local government attorneys and manufacturers on what constitutes reasonable security measures. In the meantime, manufacturers must forge ahead on their own—hopefully with the help of knowledgeable privacy counsel!