Bloomberg Law

Professional Perspective

California's New IoT Cybersecurity Law: A Guide for Business

Shawn C. Helms, Michael G. Morgan, Jason D. Krieser , and Brian M. Long, McDermott Will & Emery

California's New IoT Cybersecurity Law: A Guide for Business

Contributed by Shawn C. Helms, Michael G. Morgan, Jason D. Krieser, and Brian M. Long, McDermott Will & Emery

Beginning in Jan. 2020, an important California cybersecurity law prohibits default passwords and mandates reasonable security features in connected devices. Affected companies should be changing their products and processes to ensure compliance.

Along with the California Consumer Privacy Act of 2018, the California Legislature passed SB 327 (also known as CA Civ Code § 1798.91.04–06 (2018)). This law requires "manufacturer[s]" of "connected devices," often referred to as internet of things devices, sold in California to provide reasonable security features for those devices, prevent hackers from modifying them, and provide either a unique password for each device or require a user set password before the first use.

Although this law has been overshadowed by the CCPA, partially because the law excludes a private right of action, it imposes some important security requirements for IoT manufacturers.

Requirements

The new law provides that a manufacturer of a connected device shall equip the device with a reasonable security feature or features that are:

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

As a result, a manufacturer of a connected device must select security features that are based on the type of device and the type of information stored on the device. The device must not only protect its information at a reasonable level, depending on the type of information, but it must also protect itself from unauthorized use or modification. Here the law seems to be trying to protect IoT devices from being compromised and participating in botnets where they can cause damage to other devices or even the internet infrastructure.

Further, the law specifies for "a connected device … equipped with a means for authentication outside a local area network" a reasonable security features is deemed met if the preprogrammed password is unique to each device manufactured, and the device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.

Thus, connected devices in California can no longer be shipped with a default password that is the same on each device. Either the devices must have unique default passwords or users must be required to set their own password or authentication mechanism before the device is first used. This will be a major change for many IoT manufacturers.

Corporate Compliance

Three questions should be asked to determine if this law applies to a situation:

- Is the device a "connected device" as defined by the law?
- Is the device maker a "manufacturer" as defined in the law?
- Do any of the law's exceptions apply?

Connected Device

The law defines a connected device as "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address." This broad definition includes any physical object as long as it is capable of connecting to the internet. This broad definition clearly targets IoT devices. Any object that has built in connectivity is in scope. This includes smart appliances, newer cars with network connectivity, and traditional computers. It also includes Bluetooth-enabled gadgets such as wireless headphones and heart monitors if the data they consume is capable of being connected directly or indirectly to the internet through a mobile device or other method.

Manufacturer

The law defines a manufacturer as "the person who manufactures, or contracts with another person to manufacture on the person's behalf, connected devices that are sold or offered for sale in California." Manufacturer is defined broadly, and not just as the person who actually fabricates the device, but includes persons who contract for someone else to manufacture the device. Also, the device must be sold or offered for sale in California. The statute does not require that the manufacturer must be the one who offers or sells the device in California. Given the size and economic reach of California, it is safe to say most IoT devices will have sales in California.

The law excludes from the definition of a manufacturer a person whose contract to manufacturer is "only to purchase a connected device, or only to purchase and brand a connected device." Thus, merely contracting for a custom connected device, even if that contract includes branding, does not make a person a manufacturer. On closer examination, this does not seem to be a very broad exclusion. Although makers of devices may typically contract for the creation of a specific network component to be added to their device, this exception only applies if the device is not sold or offered for sale in California.

For example: a maker of refrigerators who contracts for the creation of a network module to add smart features to the refrigerator could be exempt from the definition if the network modules were only purchased and branded. But once the resulting refrigerator is sold or offered for sale in California, the refrigerator maker becomes a manufacturer under this law.

Exceptions

The law contains several notable exceptions to its application:

- No duty of a manufacturer related to user installed software
- No duty for a mere seller of a connected device
- No duty of a manufacturer to prevent user from having full control of the connected device
- No application to connected devices subject to federal security requirements
- No application to any health providers, business associates, or other persons subject to HIPAA or CMIA for activities regulated by those acts

How to Comply

If SB 327 applies to your company, what is the roadmap to compliance? First, review all your products and determine if a connected device allows users to login (or authenticate) to the device from outside of a local area network. If this is the case, then the law prescribes at least one security feature. The manufacturer must configure the device with a unique password, or the device must force the user to set a password before the device is used. This means that the typical practice of shipping devices with a default password and instructions on how to change it falls short of meeting this requirement.

Second, even for devices that do not authenticate outside of a local network, (such as many Bluetooth devices such as headphones), a risk analysis should be performed to determine the type of information that the device contains or can access, and the risk of misuse, or destruction of the device itself. This risk assessment should then identify controls that would be reasonable to protect the information and the device. The risk assessment should recommend controls to

manage risk based on threats, vulnerabilities, likelihoods, and impacts observed. Reasonable controls should take a cost/benefit approach to the protection of the information and the device.

Consequences of Violating This Law

First, the California attorney general or other state-employed attorneys have rights to enforce this law, but it is not known how active enforcement will be. Second, even though the law has no private right of action and thus private plaintiffs cannot bring actions directly under this law, they could conceivably make a tort/negligence claims against product manufacturers. The enactment of this law may provide plaintiffs with a standard of reasonableness that plaintiffs can use to show a breach of duty under negligence.