California has another privacy law that took effect on January 1, 2020 and it’s not the California Consumer Privacy Act (CCPA). This privacy law regulates Internet of Things (IoT) connected devices. **SB 327** was enacted in 2018 and became effective on January 1, 2020. The California IoT law requires manufacturers of connected devices to equip the device with a reasonable security feature or features that are all of the following:

- appropriate to the nature and function of the device;
- appropriate to the information the device may collect, contain, or transmit; and,
- designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

So which manufacturers must comply with this new law and what is considered a connected device?

A manufacturer is defined 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. This seems clear enough, if you manufacture a connected device that is sold or offered for sale in California, the California IoT law applies.

What is a connected device?

A connected device means 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. Smart phones, watches, speakers, wearable devices, televisions, thermostats, doorbells — the list is almost endless — are all examples connected devices.

What is a reasonable security feature?

The law states it shall be deemed a reasonable security feature if either of the following requirements are met:

(1) The preprogrammed password is unique to each device manufactured; or

(2) The device contains a security feature that requires a use to generate a new means of authentication before access is granted to the device for the first time.

California joins Oregon as one of two states that require reasonable security features for IoT devices. For more information on the Oregon IoT law, see our previously blog post here. Both of these laws mean that manufacturers must incorporate these security measures into connected devices. As a practical matter, these security features mean that IoT devices will be less vulnerable to attack since they will no longer work with the “generic” default password set by a manufacturer.

Copyright © 2021 Robinson & Cole LLP. All rights reserved.

Source URL: https://www.natlawreview.com/article/iot-manufacturers-what-you-need-to-know-about-california-s-iot-law