Akin®

California's IoT Law to Take Effect January 1, 2020

December 12, 2019

Reading Time : **1 min**

By: Rebecca Kocsis (Legal Project Analyst)

The law requires all connected devices sold or offered for sale in California to be equipped with "reasonable security" measures. The law defines "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." Such a device may include copy machines, printers, fax machines, televisions, Bluetooth headsets, keycard readers, "smart" light bulbs, personal fitness monitors, medical diagnostic equipment and a host of other devices.

In order to be complaint with the new law, IoT device manufacturers—including companies that contract with manufacturers—must equip each connected device with a "reasonable security feature or features" that are appropriate to the device's nature and function; are appropriate to the information that the device may collect, contain or transmit; and that are designed to protect the device and information contained therein from unauthorized access, destruction, use, modification or disclosure. This requirement is presumed to be satisfied if the device is equipped with a "means for authentication outside a local area network" and comes with a preprogrammed unique password or "requires a user to generate a new means of authentication before access is granted to the device for the first time."

The law does not provide a private right of action, and instead delegates enforcement to the California Attorney General (AG) and other local prosecutors. Unlike the CCPA, the IoT law grants city attorneys, county counsel and district attorneys the right to prosecute violations, along with the AG. This could open the possibility down the road of local prosecutors partnering with outside counsel to bring cases under the law. The law does not specify what

types of penalties can be sought, what the maximum penalties are or whether the enforcement authorities must prove actual harm to consumers prior to seeking penalties.

Manufacturers should re-familiarize themselves with the law's requirements in advance of the approaching January 1, 2020, implementation date and keep watch over developments in similar measures that are pending in other states.

Categories

Cybersecurity, Privacy & Data Protection

Privacy & Cybersecurity