CALIFORNIA AND THE UK TAKE THE LEAD IN SECURING INTERNET OF THINGS (IOT) DEVICES

PUBLICATION, *PENNSYLVANIA BAR ASSOCIATION* - CHASE J. WRIGHT, SEPTEMBER 18, 2019

CALIFORNIA AND THE UK TAKE THE LEAD IN SECURING INTERNET OF THINGS (IOT) DEVICES

by Chase J. Wright

Set to take effect on January 1, 2020, Senate Bill 327 and Assembly Bill 1906, together, require that manufacturers of internet-connected devices increase their security capabilities to better protect consumer data transmitted from those devices. The new California legislation, signed into law on September 28, 2018 by then-Governor Jerry Brown, will have wide-sweeping effects on the sale of Internet of Things (IoT) devices, impacting hundreds of thousands of everyday products.

The legislation applies to manufacturers of "connected devices" that are sold or offered for sale in California. Because governments around the world are starting to realize the immediate need for enhanced security measures on IoT devices, the California legislation is likely to be regarded as benchmark legislation to be used as a guide when implementing similar legislation in other states and around the globe.

This California legislation will be rolled-out on the same day as the California Consumer Privacy Act of 2018 (CCPA). The two laws are similar in purpose, but the focus of the IoT legislation is on the security of the actual products, whereas the CCPA mandates specific requirements on businesses collecting consumer information.

Under the legislation, a "connected device" (commonly referred to as IoT devices) is defined as "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an [IP] address or Bluetooth address." In general, an IoT device is a device that can connect wirelessly to a network and is capable of transmitting data. In terms of sophistication, these devices extend to far inferior devices than smartphones, computers, and tablets. Rather, IoT devices also include smart TVs, home thermostats, home security cameras, doorbells, refrigerators, toys, speakers, wearable devices, and myriad other devices that can connect wirelessly to local and external networks. With smart homes and smart vehicles now mainstream, almost any consumer product can be (or has already been) transformed into an IoT device. Reports indicate that by next year, over 20 billion IoT devices will exist globally, with those numbers expected to climb exponentially over the next decade.

Because of the limitless use of IoT devices and the historically poor reputation of security to protect data collected by those devices, the California law is seen as a leap in the right direction by data security experts; however, many argue that the law does not go far enough.

As-is, the law requires that IoT manufacturers equip such devices with a "reasonable security feature or features" that are:

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

The law provides two explicit means to satisfy the "reasonable security feature" for devices that are able to be authenticated outside of a local area network (i.e., any device that can connect to the Internet or Bluetooth). The first means to satisfy the standard is by equipping the device with a pre-programmed password that is unique to each manufactured device, and the second means is requiring a user to create a personal password before accessing the device for the first time. Although these two methods would satisfy California's statutory requirements, neither method is the only applicable method to comply with the law. Many critics of the law argue that it does not go far enough for these reasons. Specifically, critics argue that use of the vague terms "reasonable" and "appropriate" give discretion to manufacturers on the type of security means to install on IoT devices, which will result in the least secure means of data protection to satisfy the law.

Regardless of the standard, this new California IoT legislation will seriously impact manufacturers of IoT devices across the United States. The first step in analyzing whether the law is applicable to your company is to determine whether your company produces "connected devices," as defined above. If your company does manufacturer such devices that connect directly or indirectly to the Internet, and those devices are sold or offered for sale in California, then this IoT legislation is applicable. Although the law does not provide a private right of action, it authorizes the California Attorney General and city, county, and district attorneys to enforce the law.

Following in California's footsteps, the United Kingdom recently proposed similar IoT security legislation that is working its way to become law. If approved, the UK legislation would mandate that:

1. IoT device passwords be unique and not resettable to any universal factory default (as is the case in the California law);
2. Manufacturers of Internet-connected devices provide a public point of contact as part of a vulnerability disclosure policy to enable issues to be reported to the manufacturer; and
3. Internet-connected devices be capable of being securely updated and manufacturers must explicitly state the minimum length of time for which a device will receive software updates.

As shown above, the proposed UK legislation goes further than the California bills and prescribes clearer standards than the more ambiguous California law. Many critics of the California legislation have proposed amending the law to mirror the UK model.

PROFESSIONALS

Chase J. Wright

CAPABILITIES

Corporate & Business