TRAUB LIEBERMAN

CYBER LAW BLOG

October 19, 2018

California Passes IoT Security Legislation

BY: Jason Taylor

On September 28, 2018, California Governor Jerry Brown signed into law California Senate Bill 327 (Cal Civ. Code § 1798.91.04), becoming the first state to pass legislation that will specifically regulate the security of connected devices. The legislation will become operative on January 1, 2020.

As has been previously discussed in this blog, existing California law requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices in order to protect residents 'personal information from unauthorized access, destruction, use, modification, or disclosure. In recent months and years, however, there has been increasing concern about potential security flaws in products and devices that connect over the Internet -- the so-called "Internet of Things" (IoT).

IoT refers to a range of physical devices that connect with other devices through the Internet or over networks. The key aspects of IoT technology are a sensor connected to the Internet that stores and/or processes data remotely, typically in the cloud. Commonly recognized IoT technology includes "smart" devices such as appliances, thermostats, and other technology which are capable of being controlled remotely.

The accelerated advancement of IoT technology poses a number of concerns for consumers, considering many such devices lack basic security features common to cellular phones, computers, and other commonly used technological devices we often take for granted. The lack of security can leave consumers' personal information exposed and vulnerable.

For example, in 2017 various Bluetooth and wifi-enabled children's toys contained flaws that allowed strangers to remotely monitor and communicate with children. There have been reports that some dolls, controlled by hackers, prompted children to provide sensitive information verbally, including their addresses, parents' names, and school information that the hackers were able to record.

In August, the FBI published a warning stating that IoT devices such as routers, cameras, smart locks, and connected doors are being used as proxies for criminal activities.

In response to the potential security flaws in IoT devices, the California legislation will require manufacturers of devices that connect to the Internet to equip the device with "reasonable security features" designed to protect it as well as all of the information contained therein from unauthorized access, use, or disclosure. The California legislature expressed concern that "[a]n alarming number of internet connected devices lack even the most basic security features, rendering them vulnerable to hacking" and "many consumers are unaware or only vaguely aware of the security risks that come with using connected devices, leading them to unwittingly put sensitive information at risk."

The purpose of the additional measures is "to ensure that internet-connected devices are equipped with reasonable security measures to protect them from unauthorized access, use, destruction, disclosure, or modification by hackers."

Although “reasonable security features” as respects connected devices are not exhaustively defined, the protection must be appropriate to the nature and function of the connected device and appropriate to the information it may collect, contain, or transmit. For example, where a connected device is equipped with a means for authentication outside a local area network (LAN), it will be deemed a “reasonable security feature” if the device is equipped with a preprogrammed password that is unique from that assigned to all other devices and types of technology. In other words, manufactures can no longer equip IoT devices with default login credentials if someone would be able to log into the devices outside of a LAN. Additionally, if 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, the legislation provides that such a feature will be deemed a “reasonable security feature”.

Although California SB 327 is an important step forward, some critics have expressed concern that the legislation does not go far enough to protect against attacks on such devices and/or is otherwise too vague. Further, the statute does not provide for a private right of action and reserves to the Attorney General, a City Attorney, County Counsel, or District Attorney the exclusive enforcement authority.

Although California is the first state to regulate IoT devices through legislation, in June 2018, the United States House of Representatives’ Committee on Energy and Commerce introduced a bill entitled the State of Modern Application, Research, and Trends of IoT Act, otherwise known as the “SMART IoT Act.” The SMART IoT Act would empower the Secretary of Commerce to conduct a study of IoT devices, determine federal agency jurisdiction over IoT devices, provide regulations and resources, and report back to the House Committee within a year. Whether California’s passage of SB 327 spurs similar federal or state action remains to be seen.