NEWMEYER & DILLION LLP

TEDDY BEARS AND TOASTERS – CALIFORNIA LAW ADDRESSES SECURITY OF CONNECTED DEVICES

By: Anne J. Kelley

Anne J. Kelley

Contact

925.988.3200
Anne.Kelley@ndlf.com

Practice Areas

Construction Litigation
Insurance Law
Privacy & Data Security

California is once again on the cutting edge of internet security and data privacy laws. Governor Jerry Brown recently signed the nation's first law regulating the Internet of Things ("IoT") devices, SB 327, entitled "Information Privacy: Connected Devices." Starting on January 1, 2020, manufacturers of connected devices will be required to equip them with reasonable security features to protect the devices, and any information collected through the devices, from unauthorized access, destruction, use, modification or disclosure. These measures will be mandatory for all connected devices sold in California.

Formerly known as the "Teddy Bear and Toasters Act," SB 327 was created in an attempt to provide heightened security for "smart" devices that are capable of being connected to the internet and each other. American households use, on average, seven connected devices each day from talking teddy bears to toasters, TVs, lightbulbs, security systems and dishwashers. The so-called Internet of Things continues to expand as estimates reflect that in 2017, there were around 20 billion internet-connected devices worldwide and that this number will increase to 75 billion by 2025. These connected products contain embedded microprocessors that collect personal data and multiply the number of threat vectors for data breaches and cyberattacks.

Why Protect the IoT?

The new California law recognizes that these devices are becoming prevalent in homes, are being used by children, are often lacking in basic security features and are vulnerable to hacking and breaches. Along with the convenience and upsides of these devices comes a down side that many consumers do not consider before purchasing. The devices collect massive amounts of personal information, including picking up and recording conversations and monitoring what television shows we watch, what food we eat, where we travel, where we shop, when we are home, where our children are located, and when we sleep. Companies may share this information with advertisers, and hackers are trying to exploit it. As IoT devices proliferate, device attacks are sharply increasing, with three times as many of these attacks so far in 2018 than in all of 2017.

An example of such an attack occurred in 2016 when major websites like Twitter, Netflix, and Reddit went down after being hit with the Mirai botnet. This malware took advantage of in-home routers and security cameras with insufficient security to cause distributed denial-of-service attacks. The attack was possible because owners of the affected devices did not update the factory-default usernames and passwords, which were available on the internet to hackers.

How the New Law Protects Consumers

The new California law attempts to provide increased security to avoid such attacks and protect consumers who use connected devices. The law does not provide specifics on what security measures are required for all connected devices, and "reasonable security features" vary,

depending on the nature and function of the device and the nature of the information collected. Nonetheless, all connected devices must be designed to protect the device and information it collects from misuse.

The law does state that if an internet-connected device is equipped with a means for authentication outside a local area network, it will meet the "reasonable security" requirement if:

1. It has a preprogrammed password that is unique to each device, or
2. It contains a security feature that requires a purchaser to generate a new means of authentication before access is gained to the device for the first time.

This password security measure is aimed at preventing incidents like the Mirai botnet attack where hackers used default usernames and passwords.

Does SB 327 Go Far Enough?

Many cyber security experts believe the law is too vague and does not go far enough to protect consumers from the security risks inherent in these devices. Device manufacturers vigorously opposed the legislation, resulting in substantial revisions. The original version of the law required devices to indicate when they were collecting data and to notify consumers what type of data a device is capable of collecting. It also required manufacturers to provide direct notification and patching to consumers in the event of a breach and required a manufacturer to obtain consumer consent before collecting or transmitting certain information.

This law, in contrast to the recent California Consumer Privacy Act, does not have a private right of action and is only enforceable by the state. However, if a connected device manufacturer fails to maintain "reasonable security measures" and a data breach occurs, the manufacturer could be in violation of the California Consumer Privacy Act, and could face exposure to private litigation as well as regulatory action.

As California is such a large market, the new law is expected to be a de facto national standard for IoT manufacturers that offer their internet-connected devices for sale in California. Although some argue that the law does not go far enough, many believe that it is a first step towards greater security for IoT devices and that the law will engender national discussion for stronger legislation at both the state and federal level.

Anne Kelley is a partner in Newmeyer & Dillion's Walnut Creek office where she passionately advises businesses in the areas of cyber security, cyber insurance and data privacy issues, including compliance with the recent CCPA of 2018. With over three decades of experience advising policyholders on complex insurance coverage matters and litigating coverage matters in state and federal court, she brings that experience to the arena of cyber insurance coverage. You can contact Anne at anne.kelley@ndlf.com.

ABOUT NEWMEYER & DILLION LLP

For almost 35 years, Newmeyer & Dillion has delivered creative and outstanding legal solutions and trial results for a wide array of clients. With over 70 attorneys practicing in all aspects of business law, privacy & data security, employment, real estate, construction, insurance law and trial work, Newmeyer & Dillion delivers legal services tailored to meet each client's needs. Headquartered in Newport Beach, California, with offices in Walnut Creek, California and Las Vegas, Nevada, Newmeyer & Dillion attorneys are recognized by The Best Lawyers in America©, and Super Lawyers as top tier and some of the best lawyers in California, and have been given Martindale-Hubbell Peer Review's AV Preeminent® highest rating.

For additional information, call 949.854.7000 or visit www.ndlf.com.