Legal Opinion Letter

Vol. 27 No. 20 December 7, 2018

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

Internet-of-Things Security Standards: Will States Follow California's Lead or Look Across the Pond for Guidance?

by H. Michael O'Brien

In September 2018, California passed SB-327, the first law addressing growing concerns over cybersecurity for the burgeoning market of consumer Internet-of-Things (IoT) devices.

The law appears, in part, to be a response to the October 2016 Mirai "distributed denial of service" (DDoS) attack that used tens of thousands of weakly secured internet-connected consumer devices, including routers and home-security cameras. The malware was used to mount a botnet attack that shut down large swaths of the internet on the U.S. Eastern Seaboard. Lawmakers and other interested stakeholders have sought to identify preventative measures to protect internet-connected consumer devices from hackers. The more than five million new devices coming on line each day and forecasts of up to 20–25 billion devices connected to the internet by 2020 evince the need for laws and voluntary standards to mitigate potential threats.

SB-327 takes effect on January 1, 2020. The law will require manufacturers to equip connected devices with "reasonable security features" that are appropriate to (1) the nature and function of the device and (2) the information it may collect, contain, or transmit. The "reasonable security feature" can be achieved by a "preprogramed password … unique to each device" or 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." These security features are to be "designed to protect the device and any information therein from unauthorized access, destruction, use, modification or disclosure."

Is California's SB-327 the answer to achieving the goal of a threshold level of cybersecurity for consumer-based IoT devices? Or is it a temporary fix or perhaps a hindrance? Given the many contributing factors involved, the answer is unclear.

Source of the Problem

The fundamental problem with consumer-based internet-connected devices is that too many of them provide little to no cybersecurity from the outset. Their manufacturers simply don't place a high enough premium on cybersecurity, neglecting or willfully failing to "bake it in" at the design stage. Moreover, consumers are unlikely to change the factory default settings for administrators (*i.e.*, users) and passcodes. Some devices have limited computing power, making cybersecurity updates and patches impractical. One or more of these factors make IoT devices and networks easy targets for hackers who seek to infiltrate them, harvest personal data or, as with the Mirai botnet, launch a DDoS attack.

Some SB-327 commentators have suggested that the law is a minimal, perhaps futile gesture that falls short of achieving robust cybersecurity for IoT devices. Its ultimate impact, however, may be much more profound.

H. Michael O'Brien is a Partner with Wilson Elser in the firm's White Plains, NY office, where he co-chairs the Product Liability, Prevention & Government Compliance practice and leads the Internet of Things aspects of Information Governance.

Manufacturers will first need to decide which manner of implementing "reasonable security features" to select. Other than providing the two previously noted choices, the law offers little guidance. Manufacturers also must decide whether the same "reasonable security features" they choose for compliance with California's law will become the default selection for all devices sold nationwide. Since California's law is currently unique, creating one security standard for all devices sold in the U.S. seems a simple and prudent course of action. However, when other states decide to enact their own IoT cybersecurity laws, the prospect of a nationwide patchwork of varying state-law requirements could hinder the development of the IoT marketplace and create an environment that fosters litigation.

Fortunately, SB-327 specifically prohibits private rights of action by consumers, instead reserving enforcement to the California Attorney General, city attorneys, county counsel, or district attorneys. This provision seems designed to eliminate private class-action lawsuits or individual consumer actions seeking damages under the law. It also is possible that SB-327 could be used by plaintiffs in lawsuits brought in other states as a cudgel against manufacturers for failing to conform to its provisions and leaving consumers in those states vulnerable to hacks of their devices.

The UK Model

This past October the United Kingdom published its own voluntary "Code of Practice for Consumer IoT Security" for manufacturers of smart home devices. The Code was issued by the Department for Digital Culture, Media & Sport (DCMC) and the National Cyber Security Centre (NCSC). It comprises 13 guidelines and represents what is widely considered "good practice in IoT security."

Unlike California's SB-327, the UK Code is voluntary and "outcome-focused" rather than prescriptive, giving organizations the flexibility to innovate and implement security solutions appropriate for their products. The Code is also designed to be complementary to and supportive of private security efforts and relevant published cybersecurity standards "being developed from industry and international organizations."

Similarities exist, however. For instance, both the Code guidelines and California's SB-327 require all IoT device passwords to be unique and not "resettable" to any factory default setting. One must consider, however, that though both have provisions that focus on protection of consumer data and the ease with which personal data can be deleted, the relevant language in SB-327 tends to be quite vague, while the similar language in the Code is quite clear.

Additionally, the Code is more expansive than SB-327. The guidelines unique to the Code include those that suggest IoT makers do the following: implement a vulnerability disclosure policy; keep software updated; securely store credentials and security-sensitive data; communicate securely; minimize exposed attack surfaces; ensure software integrity; make systems resilient to outages; monitor system telemetry data; make installation and maintenance of devices easy; and validate input data.

Take Aways

One cannot forecast with certainty whether SB-327 will be effective at inspiring IoT device makers to enhance their products' cybersecurity. As noted above, IoT is rapidly becoming a significant technological force in the marketplace. As long as vulnerabilities continue to exist, in the absence of federal action or the emergence of widely accepted voluntary standards for IoT consumer-device security, more states will formulate their legislation. The California law may provide a model for other states' laws, but some may also consider incorporating the security guidelines set forth in the U.K. Code. How these developments unfold over the next several years will have the potential to significantly disrupt the IoT marketplace.

 ISBN 1056 3059