Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How New Calif. Law Will Impact Device Cybersecurity

By **Laura Stefani**
(October 18, 2018, 3:41 PM EDT)


Laura Stefani

While California's newly enacted net neutrality law is creating considerable controversy, including lawsuits filed by industry and the U.S. Department of Justice challenging California's ability to regulate net neutrality**,** another new law may add an additional layer of regulation for manufacturers of certain "internet of things" devices. The law, which will take effect on Jan. 1, 2020, requires specific types of cybersecurity protections for internet-connected devices — those that are capable of connecting to the internet, directly or indirectly, and are assigned IP or Bluetooth addresses.

The law will require that manufacturers of internet-connected devices that are sold in the state of California equip those devices with "reasonable security features," with the goal of protecting personal consumer information that may be contained on or transmitted by the devices. These security features must be "appropriate" both to the nature and function of the device, and to the information that it may collect, contain or transmit.

The security features also must be designed to protect the device and the information within it from "unauthorized access, destruction, use, modification, or disclosures." There is a "safe harbor" where devices are deemed compliant if they can perform authentication outside of a local area network, and either contain a unique preprogrammed password or can generate a new means of authentication prior to initial use.

The internet of things is not a new concept — utilities, for example, have used smart grid devices for decades to measure consumer energy use and system performance, and help in management of the grid. Traditionally, the Federal Communications Commission regulates the technical specifications for these wireless devices, ensuring that they operate in conformity with its requirements for using spectrum.

The Federal Trade Commission's responsibility for protecting consumer privacy includes oversight of privacy issues related to the internet of things. In 2015, for example, the FTC issued a staff report on the internet of things that provided recommendations for best practices for data security, including "reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network."[1]

The vast increase in the number of consumer devices that are connected to the internet, as well as to other devices, has raised cybersecurity concerns about connected devices, including whether the devices may be hacked to obtain consumer information, or even to obtain access or control of other devices in the home, such as a baby monitor or thermostat. Policymakers are struggling to keep up with these emerging, continually-changing cyber threats.

At the federal level, the administration is working on several fronts to develop a national cybersecurity policy, and recently issued a report on managing and reducing risks associated with botnets and other automated, distributed attacks that can pose threats for connected devices.[2] Both this report and the broader federal approach to cybersecurity consider the entire internet of things ecosystem — the devices, the communications networks and the platforms and applications that link devices, make use of data and provide the experience that consumers seek.

The report is forward-thinking, as it considers a broad-based approach to internet of things cybersecurity that includes preparing for evolving threats; implementing adaptive approaches to address those threats; encouraging information sharing between and among industry and government; engaging in international collaboration; sponsoring R&D; and providing consumer education. Specific to device manufacturers, the report suggests the use of best practices and the creation of a voluntary labeling program, but it stops short of suggesting mandatory security requirements for connected devices.

Other government agencies, such as the Department of Commerce's National Telecommunications Information Administration, have been engaged in developing a national policy on the internet of things, to include holding public meetings with a full range of stakeholders that likely will result in the development of "best practices" for industry. And the department's National Institute of Standards and Technology manages, and frequently updates, a set of standards that provide a voluntary framework for industry for cybersecurity. Even the U.S. Consumer Product Safety Commission recently held hearings and accepted public comments on whether it has a role in protecting connected consumer devices.

The California internet of things law, unlike its net neutrality law, does consider some of this federal action, with specific language that preempts devices for which there is a security requirement "under federal law, regulations, or guidance promulgated by a federal agency pursuant to its regulatory enforcement authority." The broadness of this language raises questions as to what devices may actually be subject to the specific obligations of the California law, given the considerable ongoing activity at the federal level.

Beyond uncertainty regarding the practical scope of the law, the California law addresses only one segment of the internet of things ecosystem, imposing security requirements only on device manufacturers. To be sure, devices that come with default passwords, or no password protection at all, are a major vulnerability for connected consumer devices, which in turn affects consumers' ability to protect their privacy. However, the California law explicitly does not require manufacturers to take action to prevent consumers from later modifying the software or firmware on the device, leaving open a major vulnerability for these devices.

Policy being developed at the federal level looks considers the bigger picture. One example is the emphasis that manufacturers must consider the entire lifecycle of a device, and should provide for the easy installation of security patches so that devices can be protected against new threats that arise years after manufacture.

The application and impact of California's internet of things law bears continued watching. In the short term, it may well spur more immediate and widespread changes to how consumer device manufactures equip devices with quality passwords. However, to the extent that other states follow suit and opt to adopt connected device rules or security obligations, the prospect of a conflicting patchwork of state-based internet of things requirements could hinder the development of efforts by industry and federal policymakers to develop and implement uniform security and interoperability standards that would facilitate growth, innovation and consumer adoption in a nascent part of the digital economy.

Laura A. Stefani is of counsel to Mintz Levin Cohn Ferris Glovsky and Popeo PC.

[1] www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things.

[2] www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.