HWG | HARRIS WILTSHIRE & GRANNIS LLP

CLIENT ADVISORY
May 3, 2019

Compliance Planning for California IoT Security Requirements

Adrienne Fowler, Shiva Goel, John Hodges, and Matt Miller

A recently enacted California law, SB 327, requires all Internet of Things (IoT) devices sold in the state to be equipped with reasonable security measures.[1] It is the first IoT-specific security law in the nation. The new requirements take effect **January 1, 2020**.

The new law is roughly consistent with existing oversight of IoT security, under more general laws, by the Federal Trade Commission (FTC) and state attorneys general. Nevertheless, key differences remain, and could expand as the California law is enforced and tested in the courts. SB 327 also presages a renewed focus on IoT security by other regulators. Congress, federal agencies, and other state legislatures are considering adopting similar laws, making it critical for companies to build and operationalize a compliance framework in the near-term.

Who Must Comply?

"Manufacturers" of connected devices who sell their products in California, regardless of where the product is made, will be required to include reasonable security features with their devices beginning in 2020. Importantly, SB 327 obligations extend well beyond the factory floor, defining "manufacturers" to include not only companies directly engaged in manufacturing, but also companies that "contract with" others to manufacture devices on their behalf.

What's in the Law?

Broad product coverage. The law regulates any "connected device," defined to include any device or "other physical object" that is capable of connecting to the internet (even "indirectly," such as by pairing with another device) and assigned an IP or Bluetooth address.[2]

The sweeping definition of covers a wide variety of products both conventional and new age. For example, the law plainly applies to refrigerators, air conditioners, and other household appliances that leverage internet connectivity to offer smart features, such as energy efficiency management, and to connected vehicles. Many traditional consumer electronics such as televisions and video game consoles likewise will be covered, as will newer categories of devices, like wearables and energy monitors, that are purpose-built for the IoT space.

Flexible security obligations. Under the law, connected devices must be equipped with "reasonable security features" designed to protect the device and information contained in the device from "unauthorized access, destruction, use, modification, or disclosure." Reasonable security features are defined as those "appropriate" to the "nature and function of the device" and the "information it may collect, contain, or transmit."[3] Importantly, manufacturers should understand the law as an effort to protect user safety and consumer privacy—and even safeguard against threats to public safety—given the diversity of risks posed by improper access to IoT devices. Manufacturers should consider not only traditional threats to consumer privacy, but also the physical danger compromised devices present (for example, in the case of connected cars) and the ability to weaponize IoT devices into botnets.

---

1 Cal. Civil Code § 1798.91.04-.06 (enacted Sept. 28, 2018, operative Jan. 1, 2020).

2 *Id.* § 1798.91.05.

3 *Id.* § 1798.91.04(a)(1)&(2).

The statute's indefinite standards provide industry with the flexibility to pursue risk-based approaches to IoT security. However, they also will require companies to engage in an informed and dynamic approach to compliance. While California's explicit regulation of the IoT is unprecedented, the FTC and state attorneys general have already used their broad authority to regulate unfair business practices to penalize businesses that fail to take "reasonable steps" to secure connected devices.[4] This pre-existing enforcement framework will help guide companies preparing for SB 327. Additionally, companies will need to stay apprised of evolving industry best practices and other forms of guidance from public, private, and non-profit standards bodies.

Initial password management requirements. SB 327 gets more specific in its guidance against weak default login credentials, which enabled the creation of a massive IoT botnet that brought down sites like Netflix, Twitter, Reddit, and CNN through a coordinated Distributed Denial of Service attack in 2017. In an attempt to prevent such attacks in the future, the law deems each of the following security features "reasonable" for devices that rely on remote authentication: (1) requiring the user to change the device's password before the first use, and (2) preprogramming each device with a unique default password.[5] This specificity goes beyond the guidance provided in FTC enforcement actions, which have recognized vulnerabilities posed by default settings without deeming reasonable any specific approach to initial password management.

Importantly, however, the statute provides no direction on how device makers should implement either approach. It also expressly disclaims any assurance that initial password management, even when implemented reasonably, will satisfy all applicable security obligations. Thus, initial password management should be understood as an additional requirement that applies to manufacturers using remote authentication—and not as a safe harbor that categorically limits their liability.

Exclusions. California's IoT law contains several exclusions, including security vulnerabilities caused by user installation of third-party software and devices already regulated by certain healthcare statutes.[6]

How Will It Be Enforced?

The California Attorney General, city attorneys, county counsels, and district attorneys enjoy exclusive authority to enforce the IoT security law.[7] Their enforcement of SB 327 has the potential to significantly expand legal risk in this area, although the impact remains to be seen. Unlike most other privacy and data security related laws, SB 327 does not specify what type of penalties officials can seek for violations, a maximum penalty amount, or factors that courts should consider when imposing penalties. Nor does it have an explicit requirement that officials prove any concrete harm to consumers before obtaining penalties. Nor does it specify the types of injunctive relief available. This lack of statutory limits may give enforcers virtual carte blanche in this space. Enforcement discretion and court-imposed limits may ultimately serve as effective guardrails.

In the meantime, companies should consider that SB 327 violations may result in significant monetary penalties and injunctive relief that prevents sales in some of the largest local consumer markets in the country. Indeed, the availability of a targeted statute may result in a willingness to pursue device manufacturers for security vulnerabilities more aggressively than permitted under existing law.

---

4 *See, e.g.*, *ASUSTeK Computer, Inc.*, Complaint, File No. 142 3156 (F.T.C. Feb. 23, 2016); *Trendnet, Inc.*, Complaint, File No. 122 3090 (F.T.C. Sept. 4, 2013); *Safetech Products, LLC* (N.Y. Att'y Gen. May 9, 2017).

5 Cal. Civil Code § 1798.91.04(b).

6 *Id.* § 1798.91.06(a).

7 *Id.* § 1798.91.06(e).

Companies also should be prepared for private litigation around unreasonable security practices to continue under California law even after SB 327 becomes effective. While SB 327 does not provide a private right of action, California consumers can sue for data breaches based on unreasonable security practices under California's unfair and deceptive acts and practices statute. Beginning in 2020, California consumers will be able to do the same under the California Consumer Privacy Act. It remains to be seen how SB 327 will affect consumer lawsuits filed under these separate provisions.

What's on the Horizon?

Other states, Congress, and federal agencies are actively considering efforts to regulate the security of IoT devices. For example, Oregon lawmakers have introduced a bill that largely mirrors California's statute.[8] Moreover, bipartisan legislation introduced in both the U.S. House and Senate would require manufacturers who sell IoT devices to the government to meet specially developed cybersecurity standards.[9] Additionally, the Consumer Product Safety Commission recently issued guidelines addressing the physical and public safety risks posed by connected devices[10] after seeking comment on the issue earlier last year.[11]

* * * *

For more information regarding the regulation of IoT, please contact any of the authors or the HWG lawyer with whom you regularly work at 202-730-1300. Our work extends far beyond security issues, into data privacy, energy efficiency, consumer product safety, and more. Further information about each author's work in this area is available at www.hwglaw.com/team.

This advisory is not intended to convey legal advice. It is circulated as a convenience and is not intended to reflect or create an attorney-client relationship as to its subject matter.

---

8 H.B. 2395, 80th Leg. (Or. 2019).

9 *See* IoT Cybersecurity Improvement Act of 2019, S. 734, 116th Cong. (2019); IoT Cybersecurity Improvement Act of 2019, H.R. 1668, 116th Cong. (2019).

10 Elliott F. Kaye, Commissioner, and Jonathan D. Midgett, *A Framework of Safety for the Internet of Things: Considerations for Consumer Product Safety*, U.S. Consumer Product Safety Commission (Jan. 31, 2019).

11 *See* John A. Hodges, *CPSC To Hold Hearing on Internet-Connected Consumer Products* (Mar. 31, 2018).