Decoding “Reasonableness” Under California’s IoT Law

April 7, 2021

The law governing Internet of Things (IoT) devices in the United States (US) is rapidly evolving. From industry specific guidelines for connected medical devices and autonomous vehicles, to more general standards such as the Internet of Things Cybersecurity Improvement Act of 2020 (Federal IoT Law), state and federal level laws are quickly changing as it relates to IoT standards, introducing new challenges for emerging technologies and new use cases for manufacturers.

Much like other areas of the law, California has been a leader in developing standards around IoT devices. In 2017, California became the first state to adopt an IoT specific cybersecurity law known as the California Internet of Things Cybersecurity Improvement Act of 2017 (California IoT Law). Codified at California Civil Code § 1798.91.04, the California IoT Act took effect on January 1, 2020 and requires manufacturers of IoT devices to equip any IoT device they manufacture with a “reasonable security” feature or features that are: (1) appropriate to the nature and function of the device; (2) appropriate to the information the device may collect, contain, or transmit; and (3) designed to protect the device and any information contained on the device from unauthorized access, destruction, use, modification, or disclosure. Oregon passed a similar bill into law shortly thereafter.

What is a “reasonable security” feature for IoT devices, and how will this standard be interpreted by the courts? Is it a static standard, or is it dynamic based on the type of organization and data at issue? This article examines this question and attempts to shed light on the concept of “reasonableness” under the California IoT law through an examination of statutory language and how “reasonable security” has been interpreted in parallel areas of the law.

California IoT Law Background

The California IoT Law applies to manufactures of connected devices. A manufacturer is defined as a person who manufactures, or contracts with another person to manufacture on the person’s behalf, connected devices that are sold or offered for sale in California. A connected device is defined as any device, or other physical object, that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address. Smart phones, watches, speakers, wearable devices, televisions, thermostats, could all be considered connected devices.

What Is “Reasonable Security”?

The California IoT Law does not define the term “reasonable” as it relates to device security. The law does, however, provide some guidelines as to what would be considered “reasonable.” For example, the device security features must be: (1) appropriate to the nature and function of the device; (2) appropriate to the information the device may collect, contain, or transmit; and (3) be designed to protect the device and any information contained therein from

unauthorized access, destruction, use, modification, or disclosure. For those devices that are equipped with a means for authentication outside a local area network, it is deemed also a “reasonable security feature” if either of the following requirements are met: (1) the preprogrammed password is unique to each device manufactured; and (2) 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.

In addition to these statutory requirements, what else could be considered “reasonable” under California law? To answer this question, it’s important to look elsewhere in California law. The California IoT Law is not the first to use the phrase “reasonable security.” Indeed, the same phrase is used under the California Consumer Protection Act of 2018 (CCPA), which limits the private right of action to only those instances where the underlying business fails to maintain “reasonable” security around a California resident’s personal information. The CCPA statute and its amendments do not define the phrase “reasonable security.” Nor do the CCPA regulations promulgated by the Attorney General (AG). In fact, in response to public comments provided during the CCPA regulatory drafting process, the AG noted that given the “wide-range of factual situations and different industries, as well as the need for allowing for technological advancements,” “it would be too limiting to prescribe reasonable security measures” for the purposes of the CCPA. Instead, the AG advises businesses to consult with counsel, industry standards, and technical experts for more guidance.

In 2016, the AG shed some light on what “reasonable security“ may mean under the California Records Act. In a report published in 2016, which analyzed then recent cases of data breaches in California, the AG stated that “reasonable security” under the California Records Act means, at a minimum, implementing all the controls that apply to an organization’s environment as set forth in the Center for Internet Security’s Critical Security Controls (“CIS Controls”). The AG stated that implementing the CIS Controls constitutes “a minimum level of security - a floor - that any organization that collects or maintains personal information should meet.” In addition, the AG further recommended organizations: (1) make multi-factor authentication available on consumer-facing on-line accounts that contain sensitive personal information; (2) consistently use strong encryption to protect personal information on laptops and other portable devices; and (3) encourage individuals impacted by a breach to place a fraud alert on their credit files.

Whether the CIS Controls would be considered reasonable in 2021 under the California IoT Law is an open question. Although the CIS Controls may have been viewed as a dominant cybersecurity framework in 2016, dozens of other frameworks are leveraged by organizations today. A number of global organizations, for example, measure themselves against the International Standards Organization (“ISO”) 27001 cybersecurity framework. Other organizations follow the NIST Cybersecurity Framework, a widely accepted 2014 Cybersecurity Framework prepared by the U.S. Department of Commerce’s National Institute of Standards and Technology (“NIST”). Organizations often also seek what’s known as “SOC 2” compliance, which is measured against the SOC 2 framework developed by the American Institute of Certified Public Accountants. Organizations may also choose to follow industry-specific standards, such as the Common Security Framework developed by the Health Information Trust Alliance (“HITRUST”), the HIPAA Security Rule, or the U.S. Transportation Services Administration 2011 Pipeline Security Guidelines or the North American Electric Reliability Corporation’s Critical Infrastructure Protection Standards.

Specific to IoT security, the Federal IoT law requires NIST to develop standards for IoT security as it relates to governmental agencies. NIST recently released draft guidance on IoT Device Cybersecurity Requirements. Whether and to what extent the NIST standard on IoT security becomes “reasonable” security, as it pertains under the California IoT Law, is an area that remains untested.

Conclusion

IoT manufactures in California must be cognizant of the California IoT Law, and examine what constitutes

“reasonable” in light of the particular device at issue. What constitutes “reasonable” as it relates to medical devices will necessarily be different than what constitutes “reasonable” as it relates to a smart TV. And the type of industry, size or organization, and type of data at issue are all critical questions.

As the law continues to develop and change in the IoT space, IoT manufacturers must be flexible and keep abreast of how the courts and regulators begin to decode the concept of “reasonable security” under the law.

Your Key Contacts

Peter Stockburger
Partner, San Diego
D +1 619 595 8018
peter.stockburger@dentons.com