JONES DAY

COMMENTARY

OCTOBER 2018

IN SHORT

The Situation: California is the first state to specifically regulate the security of connective devices, which are commonly referred to as internet of things ("IoT") devices.

The Result: The new law mandates that manufacturers that sell or offer to sell a connected device in California equip the device with reasonable security features as quantified in the law.

Looking Ahead: The new law takes effect on January 1, 2020.

On September 28, 2018, California Governor Jerry Brown signed legislation making California the first state to expressly regulate the security of connective devices, which are commonly referred to as internet of things ("IoT") devices. The new law takes effect on January 1, 2020. In contrast to existing California data privacy laws protecting only personal information, the new law aims to protect the security of both IoT devices and any information contained on IoT devices.

The law requires a manufacturer that sells or offers to sell a connected device in California to equip the device with a reasonable security feature or features that are all of the following: "(1) Appropriate to the nature and function of the device. (2) Appropriate to the information it may collect, contain, or transmit. (3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure." 2018 Cal. Legis. Serv. Ch. 886 (S.B. 327) (to be codified at Cal. Civ. Code § 1798.91.04(a)).

While the law only vaguely defines the term "security feature," it provides that, subject to the preceding requirements, a connected device equipped with a means for authentication outside a local area network will be deemed 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." S.B. 327 (to be codified at Cal. Civ. Code § 1798.91.04(b)).

The law also has a broad definition of "connected device," which 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." S.B. 327 (to be codified at Cal. Civ. Code § 1798.91.05(b)). As such, the law is not limited to mere consumer devices, but potentially includes, to the extent a device is not subject to other federal law or regulations, industrial IoT devices, retail point-of-sale devices, and health-related devices that connect to the internet and that receive an IP address or Bluetooth address.

> The law is not limited to mere consumer devices, but potentially includes, to the extent a device is not subject to other federal law or regulations, industrial IoT devices, retail point-of-sale devices, and health-related devices that connect to the internet and that receive an IP address or Bluetooth address.

The new IoT law does not provide for any private right of action, and it can be enforced only by the attorney general, a city attorney, a county counsel, or a district attorney. Along with other limitations and exclusions to its applicability, the law specifically does not apply to connected devices subject to security requirements under federal law, it does not limit law enforcement from obtaining information from connected devices (as authorized by law or pursuant to court orders), and it does not apply to anyone subject to the federal Health Insurance Portability and Accountability Act of 1996 (known as HIPAA) (Public Law 104-191) or California's Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1).

California remains active in 2018 with privacy, cybersecurity, and internet issues. In June, the governor signed the new California Consumer Privacy Act of 2018 (effective on January 1, 2020) into law, which includes detailed restrictions on the collection and sale of personal data. On September 30, the governor signed the California Internet Consumer Protection and Net Neutrality Act of 2018 into law, which aims to restore net neutrality. However, within hours of its signing, the Department of Justice filed a lawsuit against California, alleging that the new net neutrality law is an illegal attempt to frustrate federal policy,

which may delay the rollout of the new law.

THREE KEY TAKEAWAYS

1. The new law was designed to protect the security of IoT devices and the information those devices hold.
2. The law can be enforced only by the attorney general, a city attorney, a county counsel, or a district attorney, and does not provide for any right of private action.
3. The law does not apply to connected devices already subject to federal security standards.


Todd S. McClelland
Atlanta


Richard M. Martinez
Minneapolis


Jeff Rabkin
San Francisco / Silicon Valley


Frances P. Forte
Atlanta

YOU MIGHT BE INTERESTED IN: **Go To All Recommendations >>**


Jones Day Talks: What to Do When … You're Preparing Your Company for a Cyberattack


California Adopts Sweeping Consumer Privacy Law


U.S. Government Releases Report on IoT Botnets and Other Distributed Attacks


DOJ's Business Email Compromise Takedown Illustrates Pervasiveness of Internet Fraud Schemes

---

SUBSCRIBE SUBSCRIBE TO RSS

Jones Day is a global law firm with more than 2,500 lawyers on five continents. We are One Firm Worldwide℠.

Disclaimer: Jones Day's publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our "Contact Us" form, which can be found on our website at www.jonesday.com. The mailing of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the Firm.

© 2018 Jones Day. All rights reserved. 51 Louisiana Avenue, N.W., Washington D.C. 20001-2113