POLSINELLI

October 2018

California Takes the Lead in Regulating the Internet of Things

By Randall Stempler

After just recently enacting the broadest United States privacy law, the California Consumer Privacy Act of 2018, California took the lead once again by enacting a law for the Security of Connected Devices, commonly known as the Internet of Things ("IoT"). Both laws will become effective on January 1, 2020.

"Connected devices" are defined as devices that are capable of connecting to the Internet, directly or indirectly, and that are assigned an IP or Bluetooth address. This would include many smart home devices such as monitoring devices, speaker systems, and thermostats, as well as televisions, webcams, automobiles and other devices. Unlike the more sweeping Consumer Privacy Act, the Security of Connected Devices requirements are much more limited and focused on device security and not personal information.

The law applies to manufacturers of devices or those who have a device manufactured on its behalf for sale in California. Manufacturing does not include devices that are purchased for resale, even if private labeled.

The key provision of the law requires Connected devices have "reasonable security" features that are "appropriate to the nature and function of the device", the "information it may collect, contain, or transmit" and "designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure."

The law does not define "reasonable security", but it does provide that, subject to the other requirements, a "reasonable security feature" would be unique passwords or a requirement that the user generates "a new means of authentication before access is granted to the device for the first time." This is a "safe harbor" and not a specific requirement.

The law does not apply to devices subject to security requirements under federal law or regulations, such as those of the Food and Drug Administration. Also, persons subject to the Health Insurance Portability and Accountability Act ("HIPAA") or the Confidentiality of Medical Information Act (California) are not

Author:

Randall Stempler
Of Counsel
212.413.2844
rstempler@polsinelli.com

subject to this law with respect to activities regulated by those acts. In addition, providers of software or applications are not responsible for compliance with the law and manufacturers have no duty with respect to unaffiliated third-party software or applications added by a user. There is also no duty upon a manufacturer to prevent a user from modifying the software or firmware on the connected device or otherwise having full control over it.

Importantly, the law explicitly does not provide for a private right of action.

Although the language of the statute is not specific, it would be prudent for manufacturers of devices sold in California to plan on including security in the design of the devices and to, at a minimum, have or provide for unique passwords. For products that would have access to sensitive data or information, additional security measures may advisable.

The text of the law is set forth below.

> SECTION 1. Title 1.81.26 (commencing with Section 1798.91.04) is added to Part 4 of Division 3 of the Civil Code, to read:
>
> TITLE 1.81.26. Security of Connected Devices
>
> 1798.91.04. (a) A manufacturer of a connected device shall 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.
>
> (b) Subject to all of the requirements of subdivision (a), if a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature under subdivision (a) if either of the following requirements are met:
>
> (1) The preprogrammed password is unique to each device manufactured.
>
> (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.
>
> 1798.91.05. For the purposes of this title, the following terms have the following meanings:
>
> (a) "Authentication" means a method of verifying the authority of a user, process, or device to access resources in an information system.
>
> (b) "Connected device" means 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.
>
> (c) "Manufacturer" means the 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. For the purposes of this subdivision, a contract with another person to manufacture on the person's behalf does not include a contract only to purchase a connected device, or only to purchase and brand a connected device.
>
> (d) "Security feature" means a feature of a device designed to provide security for that device.
>
> (e) "Unauthorized access, destruction, use, modification, or disclosure" means access, destruction, use, modification, or disclosure that is not authorized by the consumer.
>
> 1798.91.06. (a) This title shall not be construed to impose any duty upon the manufacturer of a connected device related to unaffiliated

third-party software or applications that a user chooses to add to a connected device.

(b) This title shall not be construed to impose any duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications, to review or enforce compliance with this title.

(c) This title shall not be construed to impose any duty upon the manufacturer of a connected device to prevent a user from having full control over a connected device, including the ability to modify the software or firmware running on the device at the user's discretion.

(d) This title shall not apply to any connected device the functionality of which is subject to security requirements under federal law, regulations, or guidance promulgated by a federal agency pursuant to its regulatory enforcement authority.

(e) This title shall not be construed to provide a basis for a private right of action. The Attorney General, a city attorney, a county counsel, or a district attorney shall have the exclusive authority to enforce this title.

(f) The duties and obligations imposed by this title are cumulative with any other duties or obligations imposed under other law, and shall not be construed to relieve any party from any duties or obligations imposed under other law.

(g) This title shall not be construed to limit the authority of a law enforcement agency to obtain connected device information from a manufacturer as authorized by law or pursuant to an order of a court of competent jurisdiction.

(h) A covered entity, provider of health care, business associate, health care service plan, contractor, employer, or any other person subject to the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191) or the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) shall not be subject to this title with respect to any activity regulated by those acts.

(i) This title shall become operative on January 1, 2020.

SEC. 2. This act shall become operative only if Senate Bill 327 of the 2017–18 Regular Session is also enacted and becomes effective.

Learn more...

For questions regarding this alert or to learn more about how it may impact your business, please contact the author, a member of our **Privacy and Cybersecurity** practice, or your Polsinelli attorney.

To learn more about our **Privacy and Cybersecurity** practice, or to contact a member of our team, visit polsinelli.com/services/privacy-and-cybersecurity or visit our website at polsinelli.com.

Learn more...

For questions regarding this alert or to learn more about how it may impact your business, please contact the author, a member of our **Intellectual Property** practice, or your Polsinelli attorney.

To learn more about our **Intellectual Property** practice, or to contact a member of our team, visit polsinelli.com/services/intellectual-property or visit our website at polsinelli.com.

About this Publication