Senate Bill No. 327

CHAPTER 886

An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy.

[Approved by Governor September 28, 2018. Filed with Secretary of State September 28, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

SB 327, Jackson. Information privacy: connected devices.

Existing law requires a business to take all reasonable steps to dispose of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable. Existing law also requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Existing law authorizes a customer injured by a violation of these provisions to institute a civil action to recover damages.

This bill, beginning on January 1, 2020, would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to 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, as specified.

This bill would become operative only if AB 1906 of the 2017–18 Regular Session is enacted and becomes effective.

The people of the State of California do enact as follows:

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 Assembly Bill 1906 of the 2017–18 Regular Session is also enacted and becomes effective.

O