STATE OF NEW YORK

3973

2019-2020 Regular Sessions

IN SENATE

February 22, 2019

Introduced by Sen. GRIFFO -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology

AN ACT to amend the general business law, in relation to the security of connected devices

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. The general business law is amended by adding a new section 390-d to read as follows:

§ 390-d. Security of connected devices. 1. For the purposes of this section, 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 the state. For the purposes of this section, 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.

2. (a) A manufacturer of a connected device shall equip such device with a reasonable security feature or features that are all of the following:

(1) Appropriate to the nature and function of the device.

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD01120-01-9

(2) Appropriate to the information it may collect, contain, or transmit; and

(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 paragraph (a) of this subdivision, 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 such paragraph if either of the following requirements are met:

(1) The preprogrammed password is unique to each device manufactured; or

(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.

3. (a) This section 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 section 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 section.

(c) This section 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 section 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 section shall not be construed to provide a basis for a private right of action. The attorney general shall have the exclusive authority to enforce this section.

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

(g) This section 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) shall not be subject to this section with respect to any activity regulated by such act.

§ 2. This act shall take effect on the first of January next succeeding the date on which it shall have become a law.