

STATE OF NEW YORK

9179

IN SENATE

October 19, 2018

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

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:

1 Section 1. The general business law is amended by adding a new section
2 390-d to read as follows:

3 § 390-d. Security of connected devices. 1. For the purposes of this
4 section, the following terms have the following meanings:

5 (a) "Authentication" means a method of verifying the authority of a
6 user, process, or device to access resources in an information system.

7 (b) "Connected device" means any device, or other physical object that
8 is capable of connecting to the internet, directly or indirectly, and
9 that is assigned an internet protocol address or bluetooth address.

10 (c) "Manufacturer" means the person who manufactures, or contracts
11 with another person to manufacture on the person's behalf, connected
12 devices that are sold or offered for sale in the state. For the purposes
13 of this section, a contract with another person to manufacture on the
14 person's behalf does not include a contract only to purchase a connected
15 device, or only to purchase and brand a connected device.

16 (d) "Security feature" means a feature of a device designed to provide
17 security for that device.

18 (e) "Unauthorized access, destruction, use, modification, or disclo-
19 sure" means access, destruction, use, modification, or disclosure that
20 is not authorized by the consumer.

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

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

25 (2) Appropriate to the information it may collect, contain, or trans-
26 mit; and

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

LBD16604-01-8

1 (3) Designed to protect the device and any information contained ther-
2 ein from unauthorized access, destruction, use, modification, or disclo-
3 sure.

4 (b) Subject to all of the requirements of paragraph (a) of this subdivi-
5 sion, if a connected device is equipped with a means for authentica-
6 tion outside a local area network, it shall be deemed a reasonable secu-
7 rity feature under such paragraph if either of the following
8 requirements are met:

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

11 (2) The device contains a security feature that requires a user to
12 generate a new means of authentication before access is granted to the
13 device for the first time.

14 3. (a) This section shall not be construed to impose any duty upon the
15 manufacturer of a connected device related to unaffiliated third-party
16 software or applications that a user chooses to add to a connected
17 device.

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

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

26 (d) This section shall not apply to any connected device the function-
27 ality of which is subject to security requirements under federal law,
28 regulations, or guidance promulgated by a federal agency pursuant to its
29 regulatory enforcement authority.

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

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

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

41 (h) A covered entity, provider of health care, business associate,
42 health care service plan, contractor, employer, or any other person
43 subject to the federal Health Insurance Portability and Accountability
44 Act of 1996 (HIPAA) shall not be subject to this section with respect to
45 any activity regulated by such act.

46 § 2. This act shall take effect on the first of January next succeed-
47 ing the date on which it shall have become a law.