
A BILL FOR AN ACT

RELATING TO INFORMATION PRIVACY.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

1 SECTION 1. The legislature finds that despite the growing
2 number of devices that are connected to the internet, there is
3 no mandate to protect the users of these devices through
4 specific security measures.

5 Accordingly, the purpose of this Act is to require a
6 manufacturer of an internet connected device to equip the device
7 with reasonable security features that are:

8 (1) Appropriate to the nature and function of the device
9 regarding the information it may collect, contain, or
10 transmit; and

11 (2) Designed to protect the device and any information
12 contained therein from unauthorized access,
13 destruction, use, modification, or disclosure, as
14 specified.

15 SECTION 2. The Hawaii Revised Statutes is amended by
16 adding a new chapter to be appropriately designated and to read
17 as follows:



1 "CHAPTER

2 SECURITY OF CONNECTED DEVICES

3 § -1 Short title. This chapter may be cited as the
4 Security of Connected Devices Act.

5 § -2 Definitions. As used in this chapter, unless the
6 context clearly requires otherwise:

7 "Authentication" means a method of verifying the authority
8 of a user, process, or device to access resources in an
9 information system.

10 "Connected device" means any device, or other physical
11 object that is capable of connecting to the internet, directly
12 or indirectly, and that is assigned an internet protocol address
13 or bluetooth address.

14 "Manufacturer" means the person who manufactures, or
15 contracts with another person to manufacture on the person's
16 behalf, connected devices that are sold or offered for sale in
17 the State. For purposes of this chapter, a contract with
18 another person to manufacture on the person's behalf does not
19 include a contract only to purchase a connected device, or only
20 purchase and brand a connected device.



H.B. NO. 739

1 "Security feature" means a feature of a device designed to
2 provide a security for that device.

3 "Unauthorized access, destruction, use, modification, or
4 disclosure" means access, destruction, use, modification, or
5 disclosure that is not authorized by the consumer.

6 **§ -3 Security features of connected devices.** (a) A
7 manufacturer of a connected device shall equip the device with
8 reasonable security features to include all of the following:

- 9 (1) Appropriate to the nature and function of the device;
10 (2) Appropriate to the information it may collect,
11 contain, or transmit; and
12 (3) Designed to protect the device and any information
13 contained therein from unauthorized access,
14 destruction, use, modification, or disclosure.

15 (b) Subject to all the requirements of subsection
16 (a), if a connected device is equipped with a means for
17 authentication outside a local area network, it shall be deemed
18 a reasonable security feature under subsection (a), if
19 either of the following requirements is met:

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



H.B. NO. 739

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

4 § -4 Limitations on duties. (a) This chapter shall not
5 be construed to impose any duty:

6 (1) Upon the manufacturer of a connected device related to
7 unaffiliated third-party software or applications that
8 a user chooses to add to a connected device;

9 (2) Upon a provider of an electronic store, gateway,
10 marketplace, or other means of purchasing or
11 downloading software or applications, to review or
12 enforce compliance with this chapter; or

13 (3) Upon the manufacturer of a connected device to prevent
14 a user from having full control over a connected
15 device, including the ability to modify the software
16 or firmware running on the device at the user's
17 discretion.

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



H.B. NO. 739

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

4 (d) The duties and obligations imposed by this chapter are
5 cumulative with any other duties or obligations imposed under
6 other law, and shall not be construed to relieve any party from
7 any duties or obligations imposed under other law.

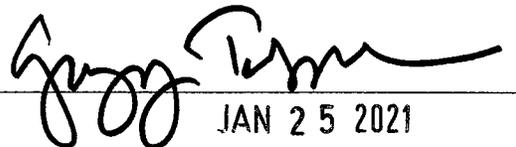
8 (e) This chapter shall not be construed to limit the
9 authority of a law enforcement agency to obtain connected device
10 information from a manufacturer as authorized by law or pursuant
11 to an order of a court of competent jurisdiction.

12 (f) A covered entity, provider of health care, business
13 associate, health care service plan, contractor, employer, or
14 any other person subject to the Health Insurance Portability and
15 Accountability Act of 1996, Public Law 104-191, shall not be
16 subject to this chapter with respect to any activity regulated
17 by it."

18 SECTION 3. This Act shall take effect upon its approval.

19

INTRODUCED BY:


JAN 25 2021



H.B. NO. 739

Report Title:

Cyber Security; Internet Connected Devices; Security Features;
Information Privacy

Description:

Requires manufacturers of connected devices to equip the devices with reasonable security features regarding information collected, unauthorized access, or the destruction or use of the devices.

The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.

