

1 H.344

2 Introduced by Representatives Rachelson of Burlington, Arsenault of
3 Williston, Burditt of West Rutland, Small of Winooski, and
4 Stone of Burlington

5 Referred to Committee on

6 Date:

7 Subject: Commerce and trade; consumer protection; data security; connected
8 devices

9 Statement of purpose of bill as introduced: This bill proposes to require that
10 connected devices sold in Vermont meet minimum security standards.

11 An act relating to adopting minimum security standards for connected
12 devices

13 It is hereby enacted by the General Assembly of the State of Vermont:

14 Sec. 1. 9 V.S.A. § 2433 is added to read:

15 § 2433. CONNECTED DEVICES; MINIMUM SECURITY STANDARDS

16 (a) A person shall not sell or deliver into this State any consumer electronic
17 product that is capable of connecting to the Internet, or to other electronic
18 products that are capable of connecting to the Internet, unless the product
19 meets the following minimum security standards:

1 (1) Encrypted communications. The product shall use encryption for its
2 network communication functions and capabilities to ensure that its
3 communications are not eavesdropped or modified in transit.

4 (2) Security updates.

5 (A) The product shall support automatic updates for a reasonable
6 period after sale, and shall be enabled by default, to ensure that when a
7 vulnerability is known, the vendor can make security updates available for
8 consumers that are verified using some form of cryptography and installed
9 seamlessly.

10 (B) An update shall not make the product unavailable to a consumer
11 for an extended period.

12 (3) Strong passwords.

13 (A) If the product uses passwords for remote authentication, it shall
14 require that strong passwords are used, including having password strength
15 requirements.

16 (B) Any nonunique default passwords shall be reset as part of the
17 device's initial setup to protect the device from vulnerability to guessable
18 password attacks.

19 (4) Vulnerability management. A vendor shall have a system in place to
20 manage vulnerabilities in the product, which shall include a point of contact for
21 reporting vulnerabilities or an equivalent bug bounty program to ensure that

1 vendors are actively managing vulnerabilities throughout the product's
2 lifecycle.

3 (5) Privacy Practices.

4 (A) The product shall have a privacy policy that is easily accessible,
5 written in language that is easily understood, and appropriate for the person
6 using the device or service.

7 (B) The vendor shall notify consumers about substantive changes to
8 the policy.

9 (C) The vendor shall disclose if it collects, transmits, or shares data
10 collected by the product for marketing purposes and shall provide the right to
11 opt-out of such practices.

12 (D) The vendor shall permit users to delete their data and account and
13 shall adopt a policy setting standard retention periods for consumer data.

14 (b) A person who violates this section commits an unfair and deceptive act
15 in commerce in violation of section 2453 of this title.

16 Sec. 2. EFFECTIVE DATE

17 This act shall take effect on July 1, 2023.