

H.630

Introduced by Representative Rachelson of Burlington

Referred to Committee on

Date:

Subject: Commerce and trade; data security; connected devices

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

An act relating to adopting minimum security standards for connected devices

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

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

§ 2433. CONNECTED DEVICES; MINIMUM SECURITY STANDARDS

(a) Requirements. A business shall not sell or deliver into this State any consumer electronic product that is capable of connecting to the internet, or to other electronic products that are capable of connecting to the internet, unless the product meets the following minimum security standards:

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

1 (2) Security updates.

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

7 (B) An update shall not make the product unavailable to a consumer
8 for an extended period of time.

9 (3) Strong passwords.

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

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

16 (4) Vulnerability management. The business shall have a system in
17 place to manage vulnerabilities in the product, which shall include a point of
18 contact for reporting vulnerabilities to ensure that vendors are actively
19 managing vulnerabilities throughout the product's lifecycle.

1 (5) Privacy practices.

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

5 (B) The business shall notify consumers about substantive changes to
6 the policy of the product.

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

10 (D) The business shall permit consumers to delete their data and
11 account that are related to the product and shall adopt a policy setting standard
12 retention periods for consumer data.

13 (b) Enforcement. A business that violates this section commits an unfair
14 and deceptive act in commerce in violation of section 2453 of this title.

15 Sec. 2. EFFECTIVE DATE

16 This act shall take effect on July 1, 2026.