S.248

Introduced by Senators Harrison and Plunkett

Referred to Committee on

Date:

Subject: Commerce and trade; consumer protection; genetic data privacy

Statement of purpose of bill as introduced: This bill proposes to require direct-to-consumer genetic testing companies and related providers to protect the genetic data information of Vermonters. The bill requires companies to limit data sharing, allows consumers to access their own data, and otherwise provides other genetic data privacy protections to consumers.

An act relating to genetic data privacy

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

Sec. 1. 9 V.S.A. chapter 61A is added to read:

CHAPTER 61A. DATA PRIVACY

Subchapter 1. Genetic Information Privacy

§ 2411. SHORT TITLE AND DEFINITIONS

(a) This subchapter shall be known, and may be cited, as the "Genetic Information Privacy Act."

(b) As used in this subchapter:

(1) "Affirmative authorization" means an action that demonstrates an intentional decision by a consumer.

(2) "Biological sample" means any material part of the human, discharge therefrom, or derivative thereof, such as tissue, blood, urine, or saliva, known to contain deoxyribonucleic acid (DNA).

(3) "Consumer" means an individual who is a Vermont resident.

(4) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice.

(5) "Direct-to-consumer genetic testing company" means an entity that:

(A) sells, markets, interprets, or otherwise offers consumer-initiated genetic testing products or services directly to consumers;

(B) analyzes genetic data obtained from a consumer, except to the extent that the analysis is performed by a person licensed in the healing arts for diagnosis or treatment of a medical condition; or

(C) collects, uses, maintains, or discloses genetic data that is:

(i) collected or derived from a direct-to-consumer genetic testing product or service; or

(ii) directly provided by a consumer.

(6) "Disclose," "disclosing," or "disclosure" means to solicit, sell, assign, transfer, give, provide, or trade, whether or not for valuable consideration.

(7) "Express consent" means a consumer's affirmative authorization to grant permission in response to a clear, meaningful, and prominent notice regarding the collection, use, maintenance, or disclosure of genetic data for a specific purpose. Express consent cannot be inferred from inaction. Agreement obtained through the use of dark patterns does not constitute express consent.

(8)(A) "Genetic data" means any data, regardless of its format, that results from the analysis of a biological sample from a consumer, or from another element enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from the analysis of the biological sample, and any information extrapolated, derived, or inferred therefrom.

(B) "Genetic data" does not include deidentified data. For purposes of this subdivision (B), "deidentified data" means data that cannot be used to infer information about, or otherwise be linked to, a particular individual, provided that the business that possesses the information:

(i) takes reasonable measures to ensure that the information cannot be associated with a consumer or household;

(ii) publicly commits to maintain and use the information only in deidentified form and not to attempt to reidentify the information, except that the business may periodically attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision (B), on the express condition that the business does not use or disclose any information reidentified in this process and destroys the reidentified information upon completion of that periodic assessment; and

(iii) contractually obligates any recipients of the information to take reasonable measures to ensure that the information cannot be associated with a consumer or household and to commit to maintaining and using the information only in deidentified form and not to reidentify the information.

(C) "Genetic data" does not include data or a biological sample to the extent that data or a biological sample is collected, used, maintained, and disclosed:

(i) exclusively for scientific research conducted by an investigator with an institution that holds an assurance with the U.S. Department of Health and Human Services pursuant to 45 C.F.R. Part 46; or

(ii) in compliance with all applicable federal and State laws and regulations for the protection of human subjects in research, including the:

(I) Common Rule, 45 C.F.R. Part 46;

(II) U.S. Food and Drug Administration regulations pursuant to 21 C.F.R. Parts 50 and 56; and

(III) Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.

(9) "Genetic testing" means any laboratory test of a biological sample from a consumer for the purpose of determining information concerning genetic material contained within the biological sample, or any information extrapolated, derived, or inferred therefrom.

(10) "Person" means an individual, partnership, corporation, association, business, business trust, or legal representative of an organization.

(11)(A) "Publicly available information" means information that is made available through federal, state, or local government records or to the general public from widely distributed media.

(B) "Publicly available information" does not include:

(i) biometric data collected by a business about a consumer without the consumer's knowledge;

(ii) information that is collated and combined to create a consumer profile that is made available to a user of a publicly available website either in exchange for payment or free of charge;

(iii) information that is made available for sale;

(iv) an inference that is generated from the information described in subdivision (ii) or (iii) of this subdivision (11)(B);

(v) any obscene visual depiction, as defined in 18 U.S.C. § 1460;

(vi) personal data that is created through the combination of personal data with publicly available information;

(vii) genetic data, unless otherwise made publicly available by the consumer to whom the information pertains;

(viii) information provided by a consumer on a website or online service made available to all members of the public, for free or for a fee, where the consumer has maintained a reasonable expectation of privacy in the information, such as by restricting the information to a specific audience; or

(ix) intimate images, authentic or computer generated, known to be nonconsensual.

(12) "Service provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is involved in the collection, transportation, and analysis of the consumer's biological sample or extracted genetic material:

(A) on behalf of the direct-to-consumer genetic testing company;

(B) on behalf of any other company that collects, uses, maintains, or discloses genetic data collected or derived from a direct-to-consumer genetic testing product or service; or

(C) that is directly provided by a consumer.

§ 2412. REQUIREMENTS

(a) Privacy terms and consent. To safeguard the privacy, confidentiality, security, and integrity of a consumer's genetic data, a direct-to-consumer genetic testing company shall:

(1) provide clear and complete information regarding the company's policies and procedures for the collection, use, maintenance, and disclosure, as applicable, of genetic data by making available to a consumer all of the following:

(A) a summary of its privacy practices, written in plain language, that includes information about the company's collection, use, maintenance, and disclosure, as applicable, of genetic data;

(B) a prominent and easily accessible privacy notice that includes, at a minimum, complete information about the company's data collection, consent, use, access, disclosure, maintenance, transfer, security, and retention and deletion practices; and

(C) a notice that the consumer's deidentified genetic or phenotypic information may be shared with or disclosed to third parties for research purposes in accordance with 45 C.F.R. Part 46; and

(2) obtain a consumer's express consent for the collection, use, and disclosure of the consumer's genetic data, including, at a minimum, separate and express consent for each of the following:

(A) the use of the genetic data collected through the genetic testing product or service offered to the consumer, including:

(i) who has access to genetic data;

(ii) how genetic data may be shared; and

(iii) the specific purposes for which the data will be collected, used, and disclosed;

(B) the storage of a consumer's biological sample after the initial testing requested by the consumer has been fulfilled;

(C) each use of genetic data or the biological sample beyond the primary purpose of the genetic testing or service and inherent contextual uses;

(D) each transfer or disclosure of the consumer's genetic data or biological sample to a third party other than a service provider, including the name of the third party to which the consumer's genetic data or biological sample will be transferred or disclosed and the intended purpose of said transfer, except that a company shall not require a consumer to expressly

consent to the actions in this subdivision (D) in order to receive the services ordered from the company by the consumer; and

(E) the marketing or facilitation of marketing to a consumer based on the consumer's genetic data or the marketing or facilitation of marketing by a third party based upon the consumer having ordered, purchased, received, or used a genetic testing product or service.

(b) Marketing exception.

(1) Subdivision (a)(2)(E) of this section does not require a direct-to-consumer genetic testing company to obtain a consumer's express consent to market to the consumer on the company's own website or mobile application based upon the consumer having ordered, purchased, received, or used a genetic testing product or service from that company if the content of the advertisement does not depend upon any information specific to that consumer. Nothing in this subdivision alters, limits, or negates the requirements of any other antidiscrimination law or targeted advertising law.

(2) Any advertisement of a third-party product or service presented to a consumer pursuant to subdivision (1) of this subsection or subdivision (a)(2)(E) of this section shall be prominently labeled as advertising content and be accompanied by the name of any third party that has contributed to the placement of the advertising. If applicable, the advertisement also shall clearly indicate that the advertised product or service, and any associated claims, have

not been vetted or endorsed by the direct-to-consumer genetic testing company.

(c) Revoking consent.

(1) A direct-to-consumer genetic testing company that is subject to the requirements in subdivision (a)(2) of this section shall provide effective mechanisms, without any unnecessary steps, for a consumer to revoke consent after it is given, at least one of which utilizes the primary medium through which the company communicates with consumers.

(2) If a consumer revokes consent pursuant to subdivision (1) of this subsection, the direct-to-consumer genetic testing company shall:

(A) honor the consumer's consent revocation as soon as practicable, but not later than 30 days after the individual revokes consent; and

(B) if the revocation is related to the storage or use of a consumer's biological sample, destroy the consumer's biological sample not later than 30 days after receipt of the revocation of consent.

(d) Data security and access.

(1) A direct-to-consumer genetic testing company shall:

(A) implement and maintain reasonable security procedures and practices to protect a consumer's genetic data against unauthorized access, destruction, use, modification, or disclosure; and

(B) develop procedures and practices to enable a consumer to easily:

(i) access the consumer's genetic data;

(ii) delete the consumer's account and genetic data, except for genetic data that is required to be retained by the company to comply with applicable legal and regulatory requirements; and

(iii) request to have and have the consumer's biological sample destroyed.

(2) Genetic data and biometric samples of consumers shall not be stored within the territorial boundaries of any country currently sanctioned in any way by the U.S. Office of Foreign Assets Control or designated as a foreign adversary under 15 C.F.R. § 7.4(a).

(3) Genetic data or biometric data of consumers shall only be transferred or stored outside the United States with the express consent of the consumer.

(e) Contracts. A contract between a direct-to-consumer genetic testing company and a service provider shall prohibit the service provider from:

(1) retaining, using, or disclosing the biological sample, genetic data, or any information regarding the identity of the consumer, including whether that consumer has solicited or received genetic testing, for a commercial purpose other than providing the services specified in the contract with the business; and

(2) associating or combining the biological sample, genetic data, or any information regarding the identity of the consumer, including whether that consumer has solicited or received genetic testing, with information the service provider has received from or on behalf of another person or persons, or has collected from its own interaction with consumers or as required by law.

(f) Discrimination. A person or public entity shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this subchapter by:

(1) denying goods, services, or benefits to the consumer;

(2) charging different prices or rates for goods or services, including through the use of discounts or other incentives, or imposing penalties;

(3) providing a different level or quality of goods, services, or benefits to the consumer;

(4) suggesting that the consumer will receive a different price or rate for goods, services, or benefits, or a different level or quality of goods, services, or benefits; and

(5) considering the consumer's exercise of rights under this subchapter as a basis for suspicion of criminal wrongdoing or unlawful conduct.

(g) Nondisclosure. Notwithstanding any other provision in this section, a direct-to-consumer genetic testing company shall not disclose a consumer's genetic data to any entity that is responsible for administering or making

decisions regarding health insurance, life insurance, long-term care insurance, disability insurance, or employment, or to any entity that provides advice to an entity that is responsible for performing those functions.

§ 2413. ENFORCEMENT

(a) A direct-to-consumer genetic testing company or service provider that violates this subchapter or rules adopted pursuant to this subchapter commits an unfair and deceptive act in commerce in violation of section 2453 of this title.

(b) The Attorney General shall have the same authority under this subchapter to make rules, conduct civil investigations, bring civil actions, and enter into assurances of discontinuance against any person as provided under chapter 63 of this title.

§ 2414. APPLICABILITY

(a) The provisions of this subchapter shall not reduce a direct-to-consumer genetic testing company's duties, obligations, requirements, or standards under any applicable State and federal laws for the protection of privacy and security.

(b) In the event of a conflict between the provisions of this subchapter and any other law, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

(c) This subchapter shall not apply to any of the following:

(1) protected health information that is collected, maintained, used, or disclosed by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164, established pursuant to the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, and the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5;

(2) a covered entity governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164, established pursuant to the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, and the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, to the extent that the provider or covered entity maintains, uses, and discloses genetic information in the same manner as medical information or protected health information, as described in subdivision (1) of this subsection;

(3) a business associate of a covered entity governed by the privacy, security, and data breach notification rules issued by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164, established pursuant to the Health Insurance Portability and Accountability Act of 1996, Pub. L.

No. 104-191, and the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, to the extent that the business associate maintains, uses, and discloses genetic information in the same manner as medical information or protected health information, as described in subdivision (1) of this subsection;

(4) scientific research or educational activities conducted by a public or private nonprofit postsecondary educational institution that holds an assurance with the U.S. Department of Health and Human Services pursuant to 45 C.F.R. Part 46, to the extent that the scientific research and educational activities conducted by that institution comply with all applicable federal and State laws and regulations for the protection of human subjects in research, including the Common Rule pursuant to 45 C.F.R. Part 46, U.S. Food and Drug Administration regulations pursuant to 21 C.F.R. Parts 50 and 56, and the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g;

(5) tests conducted exclusively to diagnose whether an individual has a specific disease, to the extent that all persons involved in the conduct of the test maintain, use, and disclose genetic information in the same manner as medical information or protected health information, as described in subdivision (1) of this subsection; and

(6) genetic data used or maintained by an employer, or disclosed by an employee to an employer, to the extent that the use, maintenance, or disclosure of that data is necessary to comply with a local, State, or federal workplace health and safety ordinance, law, or regulation.

(d) Nothing in this subchapter shall be construed to affect access to publicly available information.

Sec. 2. EFFECTIVE DATE

This act shall take effect on July 1, 2026.