An Act relating to Consumer Privacy

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

Sec. 1. FINDINGS AND INTENT

Sec 2. – General Data Protections

9 V.S.A. chapter 62 is amended to read:

§ 2430 Definitions.

(_) "Biometric identifier" means unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;

(_) "Personal Information" means any information that identifies, relates to, describes, or is capable of being associated with a particular consumer, and incorporates but is not limited to Personally Identifiable Information, Brokered Personal Information, Login Credentials, and Covered Information. "Personal Information" shall be interpreted broadly.

(_) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration. This definition shall be interpreted broadly.

§ 2432 General Requirements for Collection and Use of Data

(a) A data collector that owns, licenses, maintains, or possesses personal information, shall be subject to enforcement of any law under this Chapter.

(b) Data minimization: A data collector's collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.

(c) Secondary Uses:

(1) A data collector that obtains a consumer's personal information from a source other than the consumer may not use that information for a purpose inconsistent with the purpose for which it was initially collected, nor may it use that information for a purpose inconsistent with any notice or consent involved in the initial data collection.

(2) A data collector may not retain a consumer's personal information if it is unable to determine the initial purpose, notice, or consent described in Subparagraph (c)(1).

Commented [KR1]: The BIPA Act, below, requires this definition. This is the language found in the definitions of Brokered Personal Information and PII, in this chapter. For consistency's sake, we may want to change 2430(1)(A)(vi) and (10)(A)(v) to "Biometric identifier" so everything points back to this definition.

Commented [KR2]: Thomas Weiss has pointed out that we have a number of overlapping definitions relating to personal information in Chapter 62. While there are justifiable reasons for having done so, this is an attempt to bring some consistency into the Chapter, and to not create an entirely new, inconsistent definition.

Commented [KR3]: This definition may not be absolutely necessary – this is the language from CCPA.

Commented [KR4]: From CPRA 1798.100(c). The Consumer Reports model bill proposes the following:

(a) A business that collects a consumer's personal information shall limit its collection and sharing of that information with third parties to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or is reasonably necessary for security or fraud prevention.36 Monetization of personal information shall not be considered reasonably necessary to provide a service or conduct an activity that a consumer has requested or reasonably necessary for security or fraud prevention.
(b) A business that collects a consumer's personal information shall limit its use and retention of that information to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or a related operational purpose, provided that data collected or retained solely for security or fraud prevention may not be used for operational purposes.
(c) A consumer shall have the right, at any time, to direct a business that uses personal information about the consumer to personalize advertising not to use the consumer's personal information to personalize advertising, and the business shall have the duty to comply with the request, promptly and free of charge, pursuant to regulations developed by the Attorney General. A business that uses a consumer's personal information to personalize advertising shall provide notice that consumers have the "right to opt out" of the use of their personal information to personalize advertising.

(d) Rights of Consumers: Consumers shall have the following rights with regard to their personal information: [CCPA/CPRA-based protections]

Commented [KR5]: Ideally, it would be great if we could create rights here that are consistent with the law in California.

(e) Do Not Track

Effective ____, a data collector that processes for purposes of targeted advertising, predictive analytics, tracking, or the sale of personal information; or is a data broker, shall allow consumers to exercise the right to opt out of the processing of personal information concerning the consumer for purposes of targeted advertising, predictive analytics, tracking, or the sale of personal information through a user-selected universal opt-out mechanism that meets the technical specifications established by the Attorney General.

Commented [KR6]: This is based on Colorado Privacy Act 6-1-1306(1)(a)(IV)(B)

§ 2445 Definitions. Safe destruction of documents containing personal information

Commented [KR7]: This act was adopted in 2005 and we have not had a lot of issues with compliance, particularly because the failure to comply with this law is essentially a data breach, so the notice act is applied. It has a definition called "Personal Information" which would introduce confusion given that we are introducing a new "Personal Information" definition. In order to simplify things, I propose we delete the definition from this subchapter, and just use PII (which is the operative term in the Security Breach Notice Act) in this subchapter.

Delete definition 2445(3) "Personal Information" and replace all instances of Personal Information in Section 2445 with "Personally Identifiable Information"

Sec 3. – PROTECTION OF BIOMETRIC INFORMATION

Commented [KR8]: Need to have further discussions before firming up this language. This is based on WA BIPA with some changes.

9 V.S.A. chapter 62 is amended to read:

Subchapter 6: Biometric Information

§ 244_

(a) Collection, use, and retention of biometric identifiers.

(1) A business may not collect or retain a biometric identifier without first providing clear and conspicuous notice, obtaining consent, and providing a mechanism to prevent the subsequent use of a biometric identifier.

(2) A business who collects or retains biometric identifiers must establish a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 1 year of the consumer's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

Commented [KR9]: Based on IL BIPA

(3) Notice under subparagraph (a)(1) and (a)(5)(B) must include:

(A) a description of the biometric identifiers being collected or retained;

(B) the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, or used;

(C) the third parties to which the biometric identifier may be sold, leased, or otherwise disclosed to and the purpose of such disclosure; and

(D) the mechanism by which the consumer may prevent the subsequent use of the biometric identifier.

(4) A business who has collected or stored a consumer's biometric identifier may not use, sell, lease, or otherwise disclose the biometric identifier to another business for a specific purpose unless:

(A) consent has been obtained from the consumer for the specific purpose;

(B) it is necessary to provide a product or service subscribed to, requested, or expressly authorized by the consumer, and the business has notified the consumer of: (i) the purpose and (ii) any third parties to which the identifier is disclosed to effectuate that purpose;

(C) (i) it is necessary to effect, administer, enforce, or complete a financial transaction that the consumer requested, initiated, or authorized; (ii) the third party to whom the biometric identifier is disclosed maintains confidentiality of the biometric identifier and does not further disclose the biometric identifier except as otherwise permitted under this subsection (4); and (iii) the business has notified the consumer of any third parties to which the identifier is disclosed to effectuate that purpose; or

(D) it is required or expressly authorized by a federal or state statute, or court order.

(5)(A) Consent under subparagraph (a)(1) or (a)(4)(A) must be opt-in; and may be accomplished in writing, by indicating assent through an electronic form, through a recording of verbal assent, or in any other way that is reasonably calculated to collect informed, confirmable consent;

(B) Where biometric information is collected in a physical, offline location and consent would be impossible to collect, consent is not necessary if the business posts clear and conspicuous notice of the collection at a location likely to be seen by the consumer, provides notice on its website, and complies with all other requirements of this section.

(6) A business who possesses a biometric identifier of a consumer:

(A) Must take reasonable care to guard against unauthorized access to and acquisition of biometric identifiers that are in the possession or under the control of the business;

(B) Must comply with the data security standard set forth in Section 2447 of this Chapter and

(C) May retain the biometric identifier no longer than is reasonably necessary to:

(i) Comply with a court order, statute, or public records retention schedule specified under federal, state, or local law;

(ii) Protect against or prevent actual or potential fraud, criminal activity, claims, security threats, or liability; and

(iii) Provide the services for which the biometric identifier was collected or stored.

(7) A business who collects or stores a biometric identifier of a consumer or obtains a biometric identifier of a consumer from a third party pursuant to this section may not use or disclose it in a manner that is materially inconsistent with the terms under which the biometric identifier was originally provided without obtaining consent for the new terms of use or disclosure.

(8) Nothing in this section requires an entity to provide notice and obtain consent to collect, use or retain a biometric identifier where:

(A) the biometric identifier will be used solely to authenticate the consumer for the purpose of securing the goods or services provided by the business;

(B) the biometric identifier will not be leased or sold to any third party; and

(C) the biometric identifier will only be disclosed to a third party for the purpose of effectuating subparagraph (8)(A), and the third party is contractually obligated to maintain the confidentiality of the biometric identifier and to not further disclose the biometric identifier.

(b) Enforcement.

(1)(A) The Attorney General and State's Attorney shall have authority to investigate potential violations of this subchapter and to enforce, prosecute, obtain, and impose remedies for a violation of this subchapter or any rules or regulations made pursuant to this chapter as the Attorney General and State's Attorney have under chapter 63 of this title. The Attorney General may refer the matter to the State's Attorney in an appropriate case. The Superior Courts shall have jurisdiction over any enforcement matter brought by the Attorney General or a State's Attorney under this subsection.

(B) In determining appropriate civil penalties, the Courts shall consider each instance in which a business violates this subchapter with respect to each consumer as a separate violation, and shall base civil penalties on the seriousness of the violation, the size and sophistication of the business violating the subchapter, and the business's history of respecting or failing to respect the privacy of consumers, with maximum penalties imposed where appropriate.

(C) Businesses that possess biometric identifiers of consumers that was not acquired in accordance with the requirements of this subchapter as of the effective date of this law must either obtain consent or delete the biometric information within 180 days of enactment of this law, or shall be liable for $10,000 per day thereafter until the business has complied with this subparagraph.

(2) A consumer aggrieved by a violation of this subchapter or rules adopted under this subchapter may bring an action in Superior Court for the consumer's damages, injunctive relief, punitive damages, and reasonable costs and attorney's fees. The court, in addition, may issue an award for the greater of the consumer's actual damages or $1,000 a negligent violation; or $5,000 for a willful or reckless violation.

Commented [KR10]: Whether this word should be may or shall is a question to consider.

Commented [KR11]: This is the IL Private Right of Action Language:
Sec. 20. Right of action. Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:
(1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;
(2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;
(3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and
(4) other relief, including an injunction, as the State or federal court may deem appropriate.

Commented [KR12]: This section is based on 9 VSA 2480f(b) – Fair Credit Reporting. The $100 punitive damages have been increased to $1000, and negligent violation

(c) Exclusions.

(1) Nothing in this chapter expands or limits the authority of a law enforcement officer acting within the scope of his or her authority including, but not limited to, the authority of a state law enforcement officer in executing lawful searches and seizures.

Commented [KR13]: It might make sense to include exclusions for GLBA and HIPAA compliant activities, but that's worth a discussion.

SEC. 4 – DATA BROKERS

9 V.S.A. § 2436. Notice of data broker security breaches

(a) This section shall be known as the Data Broker Security Breach Notice Act.

(b) Notice of breach.

(1) Except as otherwise provided in subsection (d) of this section, any data broker shall notify the consumer that there has been a data broker security breach following discovery or notification to the

data broker of the breach. Notice of the security breach shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification, consistent with the legitimate needs of the law enforcement agency, as provided in subdivisions (3) and (4) of this subsection, or with any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system.

(2) A data broker shall provide notice of a breach to the Attorney General as follows:

(A)(i) The data broker shall notify the Attorney General of the date of the security breach and the date of discovery of the breach and shall provide a preliminary description of the breach within 14 business days, consistent with the legitimate needs of the law enforcement agency as provided in this subdivision (3) and subdivision (4) of this subsection (b), of the data broker's discovery of the security breach or when the data broker provides notice to consumers pursuant to this section, whichever is sooner.

(ii) If the date of the breach is unknown at the time notice is sent to the Attorney General the data broker shall send the Attorney General the date of the breach as soon as it is known.

(iii) Unless otherwise ordered by a court of this State for good cause shown, a notice provided under this subdivision (2)(A) shall not be disclosed to any person other than the authorized agent or representative of the Attorney General, a State's Attorney, or another law enforcement officer engaged in legitimate law enforcement activities without the consent of the data broker.

(B)(i) When the data broker provides notice of the breach pursuant to subdivision (1) of this subsection (b), the data broker shall notify the Attorney General of the number of Vermont consumers affected, if known to the data broker, and shall provide a copy of the notice provided to consumers under subdivision (1) of this subsection (b).

(ii) The data broker may send to the Attorney General a second copy of the consumer notice, from which is redacted the type of brokered personal information that was subject to the breach, and which the Attorney General shall use for any public disclosure of the breach.

(3)(A) The notice to a consumer required by this subsection shall be delayed upon request of a law enforcement agency. A law enforcement agency may request the delay if it believes that notification may impede a law enforcement investigation, or a national or Homeland Security investigation, or jeopardize public safety or national or Homeland Security interests. In the event law enforcement makes the request for a delay in a manner other than in writing, the data broker shall document such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. A law enforcement agency shall promptly notify the data broker in writing when the law enforcement agency no longer believes that notification may impede a law enforcement investigation, or a national or Homeland Security investigation, or jeopardize public safety or national or Homeland Security interests. The data broker shall provide notice required by this section without unreasonable delay upon receipt of a written communication, which includes facsimile or electronic communication, from the law enforcement agency withdrawing its request for delay.

(4) The notice to a consumer required in subdivision (1) of this subsection shall be clear and conspicuous. A notice to a consumer of a security breach involving brokered personal information shall include a description of each of the following, if known to the data broker:

(A) the incident in general terms;

(B) the type of brokered personal information that was subject to the security breach;

(C) the general acts of the data broker to protect the brokered personal information from further security breach;

(D) a telephone number, toll-free if available, that the consumer may call for further information and assistance;

(E) advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports; and

(F) the approximate date of the data broker security breach.

(6) A data broker may provide notice of a security breach involving brokered personal information to a consumer by one or more of the following methods:

(A) written notice mailed to the consumer's residence;

(B) electronic notice, for those consumers for whom the data broker has a valid e-mail address, if:

(i) the data broker's primary method of communication with the consumer is by electronic means, the electronic notice does not request or contain a hypertext link to a request that the consumer provide personal information, and the electronic notice conspicuously warns consumers not to provide personal information in response to electronic communications regarding security breaches; or

(ii) the notice is consistent with the provisions regarding electronic records and signatures for notices in 15 U.S.C. § 7001; or

(C) telephonic notice, provided that telephonic contact is made directly with each affected consumer and not through a prerecorded message.

(c)(1) Notice of a security breach pursuant to subsection (b) of this section is not required if the data broker establishes that misuse of brokered personal information is not reasonably possible and the data broker provides notice of the determination that the misuse of the brokered personal information is not reasonably possible pursuant to the requirements of this subsection. If the data broker establishes that misuse of the brokered personal information is not reasonably possible, the data broker shall provide notice of its determination that misuse of the brokered personal information is not reasonably possible and a detailed explanation for said determination to the Vermont Attorney General. The data broker may designate its notice and detailed explanation to the Vermont Attorney General as "trade secret" if the notice and detailed explanation meet the definition of trade secret contained in 1 V.S.A. § 317(c)(9).

(2) If a data broker established that misuse of brokered personal information was not reasonably possible under subdivision (1) of this subsection, and subsequently obtains facts indicating that misuse of the brokered personal information has occurred or is occurring, the data broker shall provide notice of the security breach pursuant to subsection (b) of this section.

(d) Any waiver of the provisions of this subchapter is contrary to public policy and is void and unenforceable.

(e) Enforcement.

(1) The Attorney General and State's Attorney shall have sole and full authority to investigate potential violations of this subchapter and to enforce, prosecute, obtain, and impose remedies for a violation of this subchapter or any rules or regulations made pursuant to this chapter as the Attorney General and State's Attorney have under chapter 63 of this title. The Attorney General may refer the matter to the State's Attorney in an appropriate case. The Superior Courts shall have jurisdiction over any enforcement matter brought by the Attorney General or a State's Attorney under this subsection.

9 V.S.A § 2446 is Amended to read:

§ 2446. Annual registration

(a) Annually, on or before January 31 following a year in which a person meets the definition of data broker as provided in section 2430 of this title, a data broker shall:

(1) register with the Secretary of State;

(2) pay a registration fee of $100.00; and

(3) provide the following information:

(A) the name and primary physical, e-mail, and Internet addresses of the data broker;

(B) ~~if the data broker permits~~ the method for a consumer to opt out of the data broker's collection of brokered personal information, opt out of its databases, or opt out of ~~certain~~ sales of data;~~:~~

~~(i) the method for requesting an opt-out;~~

~~(ii) if the opt-out applies to only certain activities or sales, which ones; and~~

~~(iii) whether the data broker permits a consumer to authorize a third party to perform the opt-out on the consumer's behalf;~~

~~(C) a statement specifying the data collection, databases, or sales activities from which a consumer may not opt out;~~

~~(D) a statement whether the data broker implements a purchaser credentialing process;~~

~~(E) the number of data broker security breaches that the data broker has experienced during the prior year, and if known, the total number of consumers affected by the breaches;~~

(C~~F~~) where the data broker ~~has actual knowledge that it~~ possesses the brokered personal information of minors, a separate statement detailing the data collection practices, databases, and sales activities~~, and opt-out policies~~ that are applicable to the brokered personal information of minors; and

(D~~G~~) any additional information or explanation the data broker chooses to provide concerning its data collection practices.

(b) A data broker that fails to register pursuant to subsection (a) of this section is liable to the State for:

(1) a civil penalty of $~~50~~100.00 for each day~~, not to exceed a total of $10,000.00 for each year,~~ it fails to register pursuant to this section;

(2) an amount equal to the fees due under this section during the period it failed to register pursuant to this section; and

(3) other penalties imposed by law.

(c) A data broker that omits required information from its registration must file an amendment to include the omitted information within 5 business days of notification of the omission, and is liable to the State for a civil penalty of $1,000 per day for each day thereafter.

(d) A data broker that files materially incorrect information in its registration:

(1) is liable to the State for a civil penalty of $25,000; and

(2) if it fails to correct the false information within 5 business days after discovery or notification of the incorrect information, an additional civil penalty of $1,000 per day for each day thereafter that it fails to correct the information.

(e~~c~~) The Attorney General may maintain an action in the Civil Division of the Superior Court to collect the penalties imposed in this section and to seek appropriate injunctive relief.

9 V.S.A § 2448 – Data Broker Additional Duties

(a) **Individual Opt-Out**

(1) A consumer or their agent may request that a Data Broker do any of the following:

(i) Stop collecting the consumer's data;

(ii) Delete all data in its possession about the consumer; or

(iii) Stop selling the consumer's data.

(2) A Data Broker must establish a simple procedure for consumers to submit such a request and must comply with such a request from a consumer or a consumer's designated agent within 10 days of receiving such a request.

(3) A Data Broker must clearly and conspicuously describe the opt-out procedure in its annual registration and on its website.

(b) **General Opt-Out**

(1) A consumer their agent may request that all Data Brokers registered with the State of Vermont honor an opt-out request by filing the request with the Secretary of State.

(2) The Secretary of State shall develop an online form to facilitate the general opt-out by a consumer or a consumer's designated agent, and shall maintain a Data Broker Opt-Out List of consumers who have requested a general opt-out, with the specific type of opt-out.

(3) The Data Broker Opt-Out List shall contain the minimum amount of information necessary for a Data Broker to identify the specific consumer making the opt-out.

(4) Once every 31 days, any Data Broker registered with the State of Vermont shall review the Data Broker Opt-Out List in order to comply with the opt-out requests contained therein.

(5) Data contained in the Data Broker opt-out list may not be used for any purpose other than to effectuate a consumer's opt-out request.

(c) **Credentialing**

Every Data Broker shall maintain reasonable procedures designed to assure that the Brokered Personal Information it discloses is to be used for a legitimate and legal purpose. These procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose. Every Data Broker shall make a reasonable effort to verify the identity of a new prospective user and the uses certified by such prospective user prior to furnishing such user Brokered Personal Information. No Data Broker may furnish Brokered Personal Information to any person if it has reasonable grounds for believing that the consumer report will not be used for a for a legitimate and legal purpose.

Commented [KR14]: This language is adapted from the credentialing requirement of FCRA [15 U.S.C. § 1681e(a)]

(d) Exemption

(1) Nothing in this section applies in any manner to Brokered Personal Information that is regulated as a Consumer Report pursuant to the Fair Credit Reporting Act, if the Data Broker is fully complying with the Fair Credit Reporting Act.

SEC. 5 – Public Information

The Attorney General shall study the following question and submit a report by December 2022:

- How the term "public" has been interpreted in the context of personal information, and whether it is appropriate to exclude public information from definitions of personal information.