

SENATE BILL NO. 85
AMENDMENT IN THE NATURE OF A SUBSTITUTE
(Proposed by the Senate Committee on General Laws and Technology
on _____)
(Patron Prior to Substitute—Senator VanValkenburg)

A BILL to amend and reenact §§ 59.1-575 and 59.1-577 of the Code of Virginia and to amend the Code of Virginia by adding a section numbered 59.1-577.2, relating to Consumer Data Protection Act; social media platforms and operators; interoperability interfaces.

Be it enacted by the General Assembly of Virginia:

1. That §§ 59.1-575 and 59.1-577 of the Code of Virginia are amended and reenacted and that the Code of Virginia is amended by adding a section numbered 59.1-577.2 as follows:

§ 59.1-575. Definitions.

As used in this chapter, unless the context requires a different meaning:

"Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. For the purposes of this definition, "control" or "controlled" means (i) ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company; (ii) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or (iii) the power to exercise controlling influence over the management of a company.

"Artificial intelligence system" means any machine learning-based system that, for any explicit or implicit objective, infers from the inputs such system receives how to generate outputs, including content, decisions, predictions, and recommendations, that can influence physical or virtual environments. "Artificial intelligence system" does not include any artificial intelligence system or general purpose artificial intelligence model that is used for development, prototyping, and research activities before such artificial intelligence system or general purpose artificial intelligence model is made available to deployers or consumers.

"Authenticate" means verifying through reasonable means that the consumer, entitled to exercise his consumer rights in § 59.1-577, is the same consumer exercising such consumer rights with respect to the personal data at issue.

"Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or

characteristics that ~~is~~ *are* used to identify a specific individual. "Biometric data" does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

"Business associate" means the same meaning as the term established by HIPAA.

"Child" means any natural person younger than 13 years of age.

"Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.

"Consumer" means a natural person who is a resident of the Commonwealth acting only in an individual or household context. ~~It~~ *"Consumer"* does not include a natural person acting in a commercial or employment context.

"Contextual data" means any information provided by a user to an artificial intelligence system over multiple sessions and any context associated with such user's interactions with such system, including prompts, conversational histories, files, preferences, or metadata. "Contextual data" does not include the trade secrets associated with an artificial intelligence system.

"Controller" means the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data.

"Covered entity" means the same as the term is established by HIPAA.

"Decisions that produce legal or similarly significant effects concerning a consumer" means a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.

"De-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person. A controller that possesses "de-identified data" shall comply with the requirements of subsection A of § 59.1-581.

"Health record" means the same as that term is defined in § 32.1-127.1:03.

"Health care provider" means the same as that term is defined in § 32.1-276.3.

"HIPAA" means the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d et seq.).

"Identified or identifiable natural person" means a person who can be readily identified, directly or

indirectly.

"Institution of higher education" means a public institution and private institution of higher education, as those terms are defined in § 23.1-100.

"Nonprofit organization" means any corporation organized under the Virginia Nonstock Corporation Act (§ 13.1-801 et seq.) or any organization exempt from taxation under § 501(c)(3), 501(c)(6), or 501(c)(12) of the Internal Revenue Code, any political organization, any organization exempt from taxation under § 501(c)(4) of the Internal Revenue Code that is identified in § 52-41, and any subsidiary or affiliate of entities organized pursuant to Chapter 9.1 (§ 56-231.15 et seq.) of Title 56.

"Online service, product, or feature" means any service, product, or feature that is provided online. "Online service, product, or feature" does not include telecommunications service, as defined in 47 U.S.C. § 153, broadband Internet access service, as defined in 47 C.F.R. § 54.400, or delivery or use of a physical product.

"Open protocol" means a publicly available technical standard that is free from licensing fees and patent restrictions and that any social media platform or operator can use to export social graph data or contextual data to another social media platform or operator.

"Operator" means a person that makes an artificial intelligence system available for use by another person. "Operator" does not include a person that solely interacts with an artificial intelligence system through application programming interfaces, licensed services, prompting, or fine tuning, or a person that makes an artificial intelligence system freely and publicly available and has no control over the operation and provision of the service, application, or software through which a user interacts with the artificial intelligence system.

"Parent" means a parent or legal guardian of a child or minor.

"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include de-identified data or publicly available information.

"Political organization" means a party, committee, association, fund, or other organization, whether or not incorporated, organized and operated primarily for the purpose of influencing or attempting to influence the selection, nomination, election, or appointment of any individual to any federal, state, or local public office or office in a political organization or the election of a presidential/vice-presidential elector, whether or not such individual or elector is selected, nominated, elected, or appointed.

"Precise geolocation data" means information derived from technology, including ~~but not limited to~~ global

92 positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the
93 specific location of a natural person with precision and accuracy within a radius of 1,750 feet. "Precise
94 geolocation data" does not include the content of communications or any data generated by or connected to
95 advanced utility metering infrastructure systems or equipment for use by a utility.

96 "Process" or "processing" means any operation or set of operations performed, whether by manual or
97 automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure,
98 analysis, deletion, or modification of personal data.

99 "Processor" means a natural or legal entity that processes personal data on behalf of a controller.

100 "Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or
101 predict personal aspects related to an identified or identifiable natural person's economic situation, health,
102 personal preferences, interests, reliability, behavior, location, or movements.

103 "Protected health information" means the same as the term is established by HIPAA.

104 "Pseudonymous data" means personal data that cannot be attributed to a specific natural person without
105 the use of additional information, provided that such additional information is kept separately and is subject
106 to appropriate technical and organizational measures to ensure that the personal data is not attributed to an
107 identified or identifiable natural person.

108 "Publicly available information" means information that is lawfully made available through federal, state,
109 or local government records, or information that a business has a reasonable basis to believe is lawfully made
110 available to the general public through widely distributed media, by the consumer, or by a person to whom
111 the consumer has disclosed the information, unless the consumer has restricted the information to a specific
112 audience.

113 "Sale of personal data" means the exchange of personal data for monetary consideration by the controller
114 to a third party. "Sale of personal data" does not include:

115 1. The disclosure of personal data to a processor that processes the personal data on behalf of the
116 controller;

117 2. The disclosure of personal data to a third party for purposes of providing a product or service requested
118 by the consumer;

119 3. The disclosure or transfer of personal data to an affiliate of the controller;

120 4. The disclosure of information that the consumer (i) intentionally made available to the general public

via a channel of mass media and (ii) did not restrict to a specific audience; or

5. The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

"Sensitive data" means a category of personal data that includes:

1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;

2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;

3. The personal data collected from a known child; or

4. Precise geolocation data.

"Social graph data" means the personal data of an identified or identifiable natural person together with any other data that represents the connections and interactions of such person within a social media platform. "Social graph data" includes the:

1. Content generated by such person;

2. Social connections of such person with other users, including such person's followers and the users that such person follows;

3. Responses of such person to the content of other users, including comments, reactions, mentions, reposts, shares, and other engagements;

4. Public profile of such person;

5. Metadata associated with the data elements in subdivisions 1 through 4; and

6. Relational references sufficient to maintain the associations among data elements described in subdivisions 1 through 4.

"Social graph data" does not include the content and responses of other users.

"Social media platform" means a public or semipublic Internet-based service or application that has users in the Commonwealth and that meets the following criteria:

1. Connects users in order to allow users to interact socially with each other within such service or application. No service or application that exclusively provides email or direct messaging services shall be considered to meet this criterion on the basis of that function alone; and

2. Allows users to do all of the following:

a. Construct a public or semipublic profile for purposes of signing into and using such service or

151 application;

152 b. Populate a public list of other users with whom such user shares a social connection within such service
153 or application; and

154 c. Create or post content viewable by other users, including content on message boards, in chat rooms, or
155 through a landing page or main feed that presents the user with content generated by other users. No service
156 or application that consists primarily of news, sports, entertainment, ecommerce, or content preselected by
157 the provider and not generated by users, and for which any chat, comments, or interactive functionality is
158 incidental to, directly related to, or dependent on the provision of such content, or that is for interactive
159 gaming, shall be considered to meet this criterion on the basis of that function alone.

160 "State agency" means the same as that term is defined in § 2.2-307.

161 "Targeted advertising" means displaying advertisements to a consumer where the advertisement is
162 selected based on personal data obtained from that consumer's activities over time and across nonaffiliated
163 websites or online applications to predict such consumer's preferences or interests. "Targeted advertising"
164 does not include:

165 1. Advertisements based on activities within a controller's own websites or online applications;

166 2. Advertisements based on the context of a consumer's current search query, visit to a website, or online
167 application;

168 3. Advertisements directed to a consumer in response to the consumer's request for information or
169 feedback; or

170 4. Processing personal data processed solely for measuring or reporting advertising performance, reach, or
171 frequency.

172 "Third party" means a natural or legal person, public authority, agency, or body other than the consumer,
173 controller, processor, or an affiliate of the processor or the controller.

174 "User" means a person not acting as an agent of a controller or processor.

175 **§ 59.1-577. Personal data rights; consumers.**

176 A. A consumer may invoke the consumer rights authorized pursuant to this subsection at any time by
177 submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A known
178 child's parent or legal guardian may invoke such consumer rights on behalf of the child regarding processing
179 personal data belonging to the known child. A controller shall comply with an authenticated consumer

request to exercise the right:

1. To confirm whether or not a controller is processing the consumer's personal data and to access such personal data;

2. To correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;

3. To delete personal data, *including social graph data processed by a social media platform and contextual data processed by an operator*, provided by or obtained about the consumer;

4. To obtain a copy of the consumer's personal data, *including social graph data processed by a social media platform and contextual data processed by an operator*, that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means, *provided that the controller shall not be required to reveal any trade secret*; and

5. To opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

B. Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to subsection A as follows:

1. A controller shall respond to the consumer without undue delay, but in all cases within 45 days of receipt of the request submitted pursuant to the methods described in subsection A. The response period may be extended once by 45 additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of any such extension within the initial 45-day response period, together with the reason for the extension.

2. If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but in all cases and at the latest within 45 days of receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision pursuant to subsection

C.

3. Information provided in response to a consumer request shall be provided by a controller free of charge, up to twice annually per consumer. If requests from a consumer are manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of

209 complying with the request or decline to act on the request. The controller bears the burden of demonstrating
210 the manifestly unfounded, excessive, or repetitive nature of the request.

211 4. If a controller is unable to authenticate the request using commercially reasonable efforts, the controller
212 shall not be required to comply with a request to initiate an action under subsection A and may request that
213 the consumer provide additional information reasonably necessary to authenticate the consumer and the
214 consumer's request.

215 5. A controller that has obtained personal data about a consumer from a source other than the consumer
216 shall be deemed in compliance with a consumer's request to delete such data pursuant to subdivision A 3 by
217 either (i) retaining a record of the deletion request and the minimum data necessary for the purpose of
218 ensuring the consumer's personal data remains deleted from the business's records and not using such retained
219 data for any other purpose pursuant to the provisions of this chapter or (ii) opting the consumer out of the
220 processing of such personal data for any purpose except for those exempted pursuant to the provisions of this
221 chapter.

222 6. *A controller that uses an artificial intelligence system provided by a third-party operator to provide*
223 *applications or services to a consumer shall promptly transmit a consumer's request to the operator with*
224 *sufficient information for the operator to execute the request and communicate about the request with the*
225 *consumer.*

226 C. A controller shall establish a process for a consumer to appeal the controller's refusal to take action on
227 a request within a reasonable period of time after the consumer's receipt of the decision pursuant to
228 subdivision B 2. The appeal process shall be conspicuously available and similar to the process for submitting
229 requests to initiate action pursuant to subsection A. Within 60 days of receipt of an appeal, a controller shall
230 inform the consumer in writing of any action taken or not taken in response to the appeal, including a written
231 explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the
232 consumer with an online mechanism, if available, or other method through which the consumer may contact
233 the Attorney General to submit a complaint.

234 ***§ 59.1-577.2. Social media platforms and operators; interoperability interfaces.***

235 A. *A social media platform shall implement a third party-accessible interoperability interface to allow a*
236 *user to share his social graph data directly with other social media platforms as he designates and enable*
237 *those social media platforms to be notified when new or updated social graph data is available. The social*
238 *media platform shall provide a mechanism by which a user may submit a request to share such data as he*

designates and shall fulfill such a request within a reasonable time frame.

B. An operator shall implement a third party-accessible interoperability interface to allow a user to share his contextual data directly with other artificial intelligence systems as he designates and enable those artificial intelligence systems to be notified when new or updated contextual data is available. The operator shall provide a mechanism by which a user may submit a request to share such data as he designates and shall fulfill such a request within a reasonable time frame.

C. To achieve interoperability as described by this section, social media platforms and operators shall:

1. Utilize an open protocol;
2. Facilitate and maintain continuous, real-time data sharing through an interoperability interface that is based on reasonable terms that do not discriminate between third parties designated by the user;
3. Establish reasonable and proportionate thresholds related to the frequency, nature, and volume of requests, where one such threshold may include a reasonable fee to be charged for such access;
4. Adopt an accessible and conspicuous method for a user to give consent for data sharing through the interoperability interface; and
5. Disclose complete, accurate, and regularly updated information describing access to the interoperability interface as required by this section.

D. Under this section, a social media platform or operator is not required to:

1. Provide access to (i) inferences, analyses, or derived data that the social media platform has generated internally about a user or (ii) trade secrets, proprietary algorithms, ranking systems, or other internal operating mechanisms;
2. Transmit data (i) that is stored or structured in a proprietary format; (ii) where no open, industry-standard format is reasonably available; and (iii) where transmitting the data would disclose proprietary information; or
3. Import data or treat imported data differently from data that is not imported.

E. No controller or processor shall collect, use, or share data obtained through the interoperability interface except for purposes of safeguarding the privacy and security of such data, delivering the services requested by the user, or maintaining interoperability of services.

F. A controller or processor that receives data shared by a user through an interoperability interface shall reasonably secure any such data.

2. That the provisions of this act shall become effective on July 1, 2027.