24104080D

SENATE BILL NO. 684

Offered January 18, 2024

A BILL to amend the Code of Virginia by adding in Title 59.1 a chapter numbered 57, consisting of sections numbered 59.1-603 through 59.1-607, relating to Online Children's Safety Protection Act established; civil penalties.

Patron—Stanley

Referred to Committee on General Laws and Technology

Be it enacted by the General Assembly of Virginia:

1. That the Code of Virginia is amended by adding in Title 59.1 a chapter numbered 57, consisting of sections numbered 59.1-603 through 59.1-607, as follows:

CHAPTER 57.

ONLINE CHILDREN'S SAFETY PROTECTION ACT.

§ 59.1-603. Definitions.

As used in this chapter, unless the context requires otherwise:

"Best interests of a child" means a child's privacy, safety, mental and physical health, access to information, freedom to participate in society, meaningful access to digital technologies, and well-being.

"Child" means a consumer who a covered entity has actual knowledge is younger than 18 years of age. For the purpose of this definition, if a covered entity chooses to conduct age estimation to determine which user is a consumer younger than 18 years of age, the covered entity shall not be considered to have actual knowledge for data processing undertaken during the period when the covered entity is estimating age or for an erroneous estimation or for data processing in the absence of reasonable evidence that a user is a consumer younger than 18 years of age.

"Collect" means the act of buying, renting, gathering, obtaining, receiving, or accessing personal data pertaining to a consumer by any means. "Collect" includes receiving information from a consumer, either actively or passively, or by observing the consumer's behavior.

"Consumer" means the same as that term is defined in § 59.1-575.

"Covered entity" means a business or organization that knowingly processes a child's personal data.

"Dark pattern" means a user interface knowingly designed with the intended purpose of subverting or impairing user decision-making or choice.

"Data protection impact assessment" means a systematic survey to assess compliance with the duty to act in the best interests of a child.

"Default" means a preselected option adopted by a covered entity for the online service, product, or feature.

"Deidentified data" means data that (i) cannot reasonably be linked to an identified or identifiable natural person or a device linked to such person and (ii) is in possession of a covered entity that (a) takes reasonable technical and administrative measures to prevent the data from being reidentified; (b) does not attempt to reidentify the data and publicly commits not to attempt to reidentify the data; and (c) contractually obligates a person to which the covered entity transfers the data to comply with the requirements of this clause (ii).

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

"Likely to be accessed by a child" means it is reasonable to expect, based on the following indicators, that an online service, product, or feature would be accessed by a child:

1. The online service, product, or feature is directed to a child, as defined in 15 U.S.C. § 6501; and

2. The online service, product, or feature is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children.

"Online service, product, or feature" does not include a telecommunications service, as defined in 47 U.S.C. § 153(53), or the delivery or use of a physical product.

"Personal data" means the same as that term is defined in § 59.1-575.

"Precise geolocation data" means data that is derived from technology and used or intended to be used to locate a consumer with precision and accuracy within a radius of 1,850 feet.

"Profile" or "profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. "Profile" or "profiling" does not include processing that does not result in some assessment or judgment about an identified or identifiable natural person.

§ 59.1-604. Duties of covered entities.

A covered entity that provides an online service, product, or feature likely to be accessed by a child shall have the following duties:

1. Within two years before any new online service, product, or feature is offered to the public on or after July 1, 2024, complete a data protection impact assessment in accordance with § 59.1-605 for an online service, product, or feature likely to be accessed by a child. In completing such data protection impact assessment, the covered entity shall consider the type of processing used in the online service, product, or feature, including new technology, and take into account the nature, scope, context, and purpose of the processing that is likely to result in high risk to a child.

2. Maintain documentation of each data protection impact assessment completed pursuant to subdivision 1 during the time period when the online service, product, or feature is reasonably likely to be accessed by a child and uses processing that is likely to result in high risk to a child.

3. Review each data protection impact assessment completed pursuant to subdivision 1 as necessary to account for any significant change to the processing operations of an online service, product, or feature.

4. Make each data protection impact assessment completed pursuant to subdivision 1 available, within a reasonable time period, to the Attorney General upon written request. Nothing in this subdivision shall be construed to require the covered entity to disclose information to the Attorney General in a manner that would disclose the covered entity's trade secrets.

5. Configure default privacy settings provided to a child by an online service, product, or feature to settings that offer a high level of privacy, unless the underlying processing enhances the child's experience of the online service, product, or feature and the covered entity offers settings to control the use of the child's data for the purpose of enhancing the child's experience. If default privacy settings meet the criteria specified under this subdivision, the default privacy settings shall not be considered a dark pattern.

§ 59.1-605. Data protection impact assessments.

A. A covered entity shall include all of the following information in a data protection impact assessment required under subdivision 1 of § 59.1-604:

1. The purpose of an online service, product, or feature provided by the covered entity;

2. The manner in which the online service, product, or feature uses a child's personal data; and

3. A determination as to whether the online service, product, or feature is designed and offered in a manner consistent with the best interests of a child who is reasonably likely to access the online service, product, or feature. In making such determination, the covered entity shall include all of the following information:

a. A systematic description of the anticipated processing operations and the purpose of the processing;

b. An assessment of the necessity and proportionality of the processing operations in relation to the purpose of the processing. For the purpose of this subdivision, a single assessment may address a set of similar processing operations that present similar risks;

c. An assessment of the risks to the rights and freedoms of a child; and

d. The measures anticipated to address the risks, including safeguards, security measures, and mechanisms, to ensure the protection of personal data and to demonstrate compliance with this chapter, taking into account the rights and freedoms of a child.

B. Notwithstanding any other provision of law, a data protection impact assessment required under subdivision 1 of § 59.1-604 shall be protected as confidential and shall not be subject to the provisions of the Virginia Freedom of Information Act (§ 2.2-3700 et seq.).

C. To the extent information contained in a data protection impact assessment required under subdivision 1 of § 59.1-604 and disclosed to the Attorney General under subdivision 4 of § 59.1-604 includes information subject to attorney-client privilege or work product protection, the disclosure shall not constitute a waiver of attorney-client privilege or work product protection.

D. A data protection impact assessment conducted by a covered entity for the purpose of compliance with any other law of the Commonwealth shall be deemed to comply with the requirements of this chapter.

§ 59.1-606. Prohibition on certain actions by covered entities.

No covered entity that provides an online service, product, or feature reasonably likely to be accessed by a child shall:

1. Use the personal data of a child likely to access the online service, product, or feature in a way that the covered entity knows is likely to result in high risk to the child on the basis of a data protection impact assessment required under subdivision 1 of § 59.1-604 if the high risk has not been suitably mitigated through measures identified in the data protection impact assessment.

2. Profile a child by default if the profiling has been identified as high risk to the child on the basis of a data protection impact assessment required under subdivision 1 of § 59.1-604 unless the high risk

has been suitably mitigated through measures identified in the data protection impact assessment. If the covered entity profiles by default, there shall be a presumption that the profiling does not violate this subdivision if (i) the covered entity can demonstrate that the covered entity has appropriate safeguards in place to protect a child; (ii) the profiling is necessary to provide the online service, product, or feature requested and only used regarding the aspects of the online service, product, or feature with which a child is actively and knowingly engaged; and (iii) the profiling enhances a child's experience on an online service, product, or feature and the covered entity offers settings to control the use of the child's data for the purpose of enhancing the child's experience.

3. Collect, retain, process, or disclose the personal data of a child in a manner that has been identified as high risk to the child on the basis of a data protection impact assessment required under subdivision 1 of § 59.1-604 unless the high risk has been suitably mitigated through measures identified in the data protection impact assessment.

4. If the end user is a child, use personal data for any reason other than a reason for which that personal data was collected, unless the covered entity can demonstrate a compelling reason that use of the personal data is in the best interests of a child.

5. Collect, sell, process, or retain the precise geolocation information of a child by default unless (i) the covered entity can demonstrate a compelling reason that such activities are in the best interests of a child or (ii) the processing enhances a child's experience of an online service, product, or feature and the covered entity offers settings to control the use of the child's data for the purposes of enhancing the child's experience.

6. Track the precise geolocation information of a child without providing notice regarding the tracking of the child's precise geolocation information.

7. Use dark patterns to knowingly lead or encourage a child to (i) provide personal data in excess of what is reasonably expected to furnish an online service, product, or feature; (ii) forgo privacy protections; or (iii) take any action that the covered entity knows is not in the best interests of a child reasonably likely to access the online service, product, or feature.

§ 59.1-607. Enforcement; civil penalties; expenses.

A. The Attorney General shall have exclusive authority to enforce the provisions of this chapter.

B. Prior to initiating any action under this chapter, the Attorney General shall provide a covered entity 90 days' written notice identifying the specific provisions of this chapter the Attorney General alleges have been or are being violated. If within the 90-day period the covered entity cures the noticed violation and provides the Attorney General an express written statement that the alleged violations have been cured and that no further violations shall occur, no action shall be initiated against the covered entity.

C. If a covered entity continues to violate this chapter following the cure period in subsection B or breaches an express written statement provided to the Attorney General under that subsection, the Attorney General may initiate an action in the name of the Commonwealth and may seek an injunction to restrain any violations of this chapter and civil penalties of no more than $2,500 per affected child for each negligent violation or no more than $7,500 per affected child for each intentional violation under this chapter. All civil penalties, expenses, and attorney fees collected pursuant to this chapter shall be paid into the state treasury and credited to the Regulatory, Consumer Advocacy, Litigation, and Enforcement Revolving Trust Fund.

D. The Attorney General may recover reasonable expenses incurred in investigating and preparing the case, including attorney fees, in any action initiated under this chapter.

E. Nothing in this chapter shall be construed as providing the basis for, or be subject to, a private right of action for violations of this chapter or under any other law.

F. Compliance by a covered entity with the federal Children's Online Privacy Protection Act, 15 U.S.C. § 6501 et seq., shall constitute compliance with this chapter for a child younger than 13 years of age.