PRINTER'S NO. 2359

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 1879 Session of 2023

INTRODUCED BY BULLOCK, GREGORY, STEELE, KINSEY, BURGOS, GUENST, MADDEN, HILL-EVANS, CERRATO, SANCHEZ, FLICK, HADDOCK, PARKER, BOYD, GERGELY, KHAN, CEPHAS, SIEGEL, ISAACSON, KUZMA, GIRAL, ABNEY, A. BROWN, FRIEL, ORTITAY, DALEY, DAWKINS, ROZZI, METZGAR AND MERCURI, DECEMBER 5, 2023

REFERRED TO COMMITTEE ON CHILDREN AND YOUTH, DECEMBER 5, 2023

AN ACT

Providing for duties of covered entities to protect the best interests of children that use online services, products or features and for data protection impact assessments; prohibiting certain actions by covered entities; and imposing penalties.

The General Assembly of the Commonwealth of Pennsylvania hereby enacts as follows:

Section 1. Short title.

This act shall be known and may be cited as the Online Safety Protection Act.

Section 2. Findings and declarations.

The General Assembly finds and declares as follows:

(1) Covered entities that develop and provide online services, products or features that children are likely to access should consider the best interests of children when designing, developing and providing that online service, product or feature.

(2) If a conflict arises between commercial interests

and the best interests of children, covered entities that develop online products, services or features likely to be accessed by children should prioritize the privacy, safety and well-being of children over commercial interests.

Section 3. Definitions.

The following words and phrases when used in this act shall have the meanings given to them in this section unless the context clearly indicates otherwise:

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

"Consumer." An individual who is a resident of this Commonwealth. The term does not include an individual acting in a commercial or employment context or as an employee, owner,

director, officer or contractor of a company, partnership, sole proprietorship, nonprofit entity or State agency whose communications or transactions with a covered entity occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit entity or State agency.

"Covered entity." A business or organization that knowingly processes a child's personal information.

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

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

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

"Deidentified data." Data that meets all of the following criteria:

(1) The data cannot reasonably be linked to an individual or a device linked to the individual.

(2) The data is in possession of a covered entity that:

(i) takes reasonable technical and administrative measures to prevent the data from being reidentified;

(ii) does not attempt to reidentify the data and publicly commits not to attempt to reidentify the data; and

(iii) contractually obligates a person to which the covered entity transfers the data to comply with the requirements of this paragraph.

"Likely to be accessed by a child." 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 (relating to definitions).

(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." The term does not include any of the following:

(1) A telecommunications service as defined in 47 U.S.C. § 153(53) (relating to definitions).

(2) The delivery or use of a physical product.

"Personal information." Information that is linked or reasonably linkable to an identified or identifiable individual. The term does not include deidentified data or publicly available information.

"Precise geolocation data." Data that is derived from a device and used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet.

"Profile." A form of automated processing of personal information that uses personal information to evaluate certain aspects relating to an individual, including analyzing or predicting aspects concerning an individual's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. The term does not include processing that does not result in some assessment or judgment about an individual.

Section 4. 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 the effective date of this paragraph, complete a data protection impact assessment in accordance with section 5 for an online service, product or feature likely to be accessed by a child. In completing the 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 under paragraph (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 under paragraph (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 under paragraph (1) available, within a reasonable time period, to the Office of Attorney General upon written request. Nothing in this paragraph shall be construed to require the covered entity to disclose information to the Office of 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 paragraph, the default privacy settings shall not be considered a dark pattern.

Section 5. Data protection impact assessments.

(a) Information.--A covered entity shall include all of the following information in a data protection impact assessment required under section 4(1):

(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 information.

(3) A determination 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 the determination under this paragraph, the covered entity shall include all of the following information:

(i) A systematic description of the anticipated processing operations and the purpose of the processing.

(ii) An assessment of the necessity and proportionality of the processing operations in relation to the purpose of the processing. For the purpose of this

subparagraph, a single assessment may address a set of similar processing operations that present similar risks.

(iii) An assessment of the risks to the rights and freedoms of a child.

(iv) The measures anticipated to address the risks, including safeguards, security measures and mechanisms, to ensure the protection of personal information and to demonstrate compliance with this act, taking into account the rights and freedoms of a child.

(b) Accessibility.--Notwithstanding any other provision of law, a data protection impact assessment required under section 4(1) shall be protected as confidential and shall not be accessible under the act of February 14, 2008 (P.L.6, No.3), known as the Right-to-Know Law.

(c) Attorney-client privilege.--To the extent information contained in a data protection impact assessment required under section 4(1) and disclosed to the Office of Attorney General under section 4(4) 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) Compliance.--A data protection impact assessment conducted by a covered entity for the purpose of compliance with any other law of this Commonwealth shall be deemed to comply with the requirements under this act.

Section 6. Prohibition on certain actions by covered entities.

A covered entity that provides an online service, product or feature reasonably likely to be accessed by a child may not take any of the following actions:

(1) Use the personal information 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 section 4(1) 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 section 4(1) if the high risk has not 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 paragraph if any of the following apply:

(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.

(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 information 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 section 4(1) if the high

risk has not been suitably mitigated through measures identified in the data protection impact assessment.

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

(5) Collect, sell, process or retain the precise geolocation information of a child by default unless any of the following apply:

(i) The covered entity can demonstrate a compelling reason that the processing is in the best interests of a child.

(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 do any of the following:

(i) Provide personal information in excess of what is reasonably expected to furnish an online service, product or feature.

(ii) Forego privacy protections.

(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.

Section 7. Penalties.

(a) Actions.--The Office of Attorney General may initiate a civil action in a court of competent jurisdiction seeking injunctive relief or a civil penalty against a covered entity that violates this act in accordance with this section. Upon a covered entity being found liable for a violation of this act by a court of competent jurisdiction, the court may issue an order:

(1) granting injunctive relief; or

(2) imposing a civil penalty 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.

(b) Remittance.--Civil penalties awarded under subsection (a) shall be remitted to the Office of Attorney General to offset the costs incurred by the Office of Attorney General in enforcing the provisions of this act.

(c) Notice.--If a covered entity has made a good faith effort to comply with the requirements under section 4, the Office of Attorney General shall provide written notice to the covered entity before initiating a civil action under subsection (a). The Office of Attorney General shall identify the specific provisions of this act that the Office of Attorney General alleges to have been or are being violated in the written notice.

(d) Cured violation.--If, within 90 days of receipt of the written notice required under subsection (c), the covered entity cures an alleged violation specified in the written notice and provides the Office of Attorney General with written evidence that the alleged violation has been cured and the covered entity has taken sufficient measures to prevent a future violation of this act, the covered entity shall not be civilly liable for the

alleged violation.

(e) Compliance with Federal law.--Compliance by a covered entity with 15 U.S.C. Ch. 91 (relating to children's online privacy protection) shall constitute compliance with this act for a child younger than 13 years of age.

Section 8. Construction.

Nothing in this act shall be construed to:

(1) provide a private right of action under this act or any other law of this Commonwealth;

(2) impose liability in a manner that is inconsistent with 47 U.S.C. § 230 (relating to protection for private blocking and screening of offensive material); or

(3) infringe on the existing rights and freedoms of a child.

Section 9. Applicability.

(a) Nonapplicability.--This act shall not apply to any of the following:

(1) An online service, product or feature that is not offered to the public.

(2) Protected health information that is collected by a covered entity or a covered entity's associate governed by the privacy, security and breach notification rules issued by the United States Department of Health and Human Services under 45 CFR Subt. A Subch. C Pts. 160 (relating to general administrative requirements) and 164 (relating to security and privacy) in accordance with the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191, 110 Stat. 1936) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, 123 Stat. 226-279 and 467-496).

(3) A covered entity governed by the privacy, security and breach notification rules issued by the United States Department of Health and Human Services under 45 CFR Subt. A Subch. C Pts. 160 and 164 in accordance with the Health Insurance Portability and Accountability Act of 1996 to the extent the covered entity maintains patient information in the same manner as protected health information under paragraph (2).

(4) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, in accordance with good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or in accordance with the human subject protection requirements of the United States Food and Drug Administration.

(b) Conflicting Federal laws.--

(1) This act shall not apply upon the effective date of a Federal law, regulation or rule or an amendment or modification to a Federal law, regulation or rule, including an amendment to 15 U.S.C. Ch. 91 (relating to children's online privacy protection), relating to any of the following:

(i) A covered entity's collection, use, retention or disclosure of personal information of an individual younger than 18 years of age.

(ii) Consent requirements for the collection, use, retention or disclosure of personal information of an individual younger than 18 years of age, including consent requirements to register for or maintain an account with an online service.

(iii) Requirements to ascertain or verify the age of an individual.

(iv) Parental settings, controls or other oversight or monitoring mechanisms.

(2) The Office of Attorney General shall submit a notice to the Legislative Reference Bureau for publication in the next available issue of the Pennsylvania Bulletin of the effective date of a Federal law, regulation or rule or an amendment or modification to a Federal law, regulation or rule specified under paragraph (1).

Section 10. Effective date.

This act shall take effect in 60 days.