STATE OF NEW YORK

4967

2023-2024 Regular Sessions

IN ASSEMBLY

February 27, 2023

Introduced by M. of A. ROZIC -- read once and referred to the Committee on Science and Technology

AN ACT to amend the general business law, in relation to enacting the New York child data privacy and protection act

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. This act shall be known and may be cited as the "New York child data privacy and protection act".

§ 2. Legislative intent. The legislature hereby finds that 95% of individuals under the age of 18 in the United States enjoy access to the Internet in their residences.

The legislature further finds that American teenagers spend seven hours and 22 minutes on average per day browsing social media, and that 53% of children will own a smartphone by the time they're 11 years of age.

The legislature recognizes that, while broadband access is a core component of modern life and critical to the ability of children and young people to feel socially, emotionally, economically, and educationally connected to the world around them, it is not without its risks and detriments.

The legislature finds, for example, that teenagers who spend between five to seven hours a day on the Internet are twice as likely to suffer from depression compared to those logged in for one hour a day.

The legislature further finds that, according to recent surveys conducted by a prominent social media platform, 34% of young adults feel uneasy when they are not online, 40.6% complain that their sleep habits have been negatively affected by social media, and 35% report being cyberbullied on the Internet.

The legislature further finds that, according to the 2021 U.S. Surgeon General Advisory on Protecting Youth Mental Health, digital public spaces are frequently designed to maximize user engagement as

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD06552-01-3

opposed to safeguarding user health, leading to negative impacts of digital technologies and social media on the mental health and well-being of adolescents.

The legislature further finds that the pitfalls of the Internet are not limited to teenagers, with young children potentially exposed to unsettling, dangerous, or age inappropriate content if not closely monitored by an adult.

The legislature further finds that young children run a higher risk of coming into contact with strangers online, inadvertently sharing personal information online, inadvertently making in-app purchases or signing contracts, terms, or conditions online, becoming subject to, witnessing, or participating in potentially harmful conduct online, or purchasing drugs and other dangerous products advertised online or sold through online platforms.

The legislature recognizes the role of lawmakers to guard against and mitigate these risks for children under the age of 18 wherever possible.

The legislature finds that, while Congress passed the landmark Children's Online Privacy Protection Act (COPPA) in 1998 limiting the collection, use, and disclosure of data collected from children under 13 years of age, requiring operators to retain such data for a limited amount of time, and restricting certain marketing to children under 13 years of age, multiple studies have found the vast majority of application developers to be out of compliance with these rules.

The legislature further finds that recent studies show at least two-thirds of applications transmit data about very young children to third party marketing companies.

The legislature further finds that President Biden recently declared the need to "strengthen privacy protections, ban targeted advertising to children, [~~and~~] demand tech companies stop collecting personal data on our children" in his 2022 State of the Union Address.

The legislature further finds that, subsequent to this address, the Federal Trade Commission announced that it will prioritize the enforcement and modernization of COPPA to "crack down on companies that illegally surveil children online".

The legislature further finds that there has been a flurry of recent legislative activity at the state, federal, and international levels to address this issue, including the California Age-Appropriate Design Code Act, the Virginia's Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, several federal proposals to strengthen and improve COPPA, and the UK's Age Appropriate Design Code.

The legislature hereby concludes that the state of New York too has a role to play in better preventing the exploitation of children's data in the modern era, and thus presents the New York Child Data Privacy and Protection Act.

§ 3. The article heading of article 39-F of the general business law, as amended by chapter 117 of the laws of 2019, is amended to read as follows:

NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION; DATA SECURITY PROTECTIONS**; CHILD DATA PRIVACY AND PROTECTION ACT**

§ 4. The general business law is amended by adding a new section 899-cc to read as follows:

§ 899-cc. New York child data privacy and protection act. 1. Definitions.

(a) "Bureau" shall mean the bureau of internet and technology in the office of the New York attorney general.

(b) "Child" or "children" shall mean a consumer or consumers under eighteen years of age.

(c) "Child user" shall mean a child accessing an online product with a device.

(d) "Data breach" shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data of child users transmitted, stored, or otherwise processed.

(e) "Data controller" or "controller" shall mean a natural or legal person which, alone or jointly with others, determines the purposes and means of processing of the personal data of child users. This includes, but is not limited to, any business, website, or platform that collects data while selling electronic advertising space on its platform tailed to any one or any aggregation of the items of personal data defined in this section. No data controller is exempt from the requirements of this article if they are processing pseudonymized data, whereby "pseudonymized" or "pseudonymization" means the processing of personal data in a manner that renders the personal data no longer attributable to a specific child user without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable child user.

(f) "Data protection impact assessment" shall mean an internal evaluation which the bureau requires entities to carry out in order to evaluate the level of risk associated with such entity's collection, retention, processing, or sale of child user data.

(g) "Online product" shall mean an online service, feature, or platform that is accessible to users with a digital device.

(h) "Personal data" or "personal data identifier" shall mean any computerized information about a child user set forth in this paragraph that is not made publicly available through federal, state or local government agencies or any publicly available information, regardless of whether it is collected for the purpose of selling or transferring it to another entity. Personal data shall mean information that identifies, relates to, describes or is reasonably linked to a particular child user, including but not limited to:

(i) physical address;

(ii) legal name;

(iii) alias;

(iv) unique personal identifier;

(v) online identifier;

(vi) internet protocol address;

(vii) e-mail address;

(viii) account name;

(ix) social security number;

(x) place of birth;

(xi) date of birth;

(xii) phone number;

(xiii) audio, visual, thermal, or olfactory data;

(xiv) medical history, records of past medical treatment, or any diagnosis of a physical or mental health condition or disability;

(xv) educational information that is not already publicly available through a local, state, or federal agency;

(xvi) real time geolocation data or stored geolocation history;

(xvii) any unique biometric data, body measurement, technical analysis or measurements collected for the purpose of allowing a child user to authenticate him or herself on a device, internet application, or web-based platform;

(xviii) names and identifying information of a child user's immediate family;

(xix) internet or any other electronic network activity, including browsing history, search history, and information regarding a child user's activity on a website or interaction with an electronic advertisement;

(xx) any other information that alone, or combined with any of the information described in this paragraph, could be reasonably used to identify an individual child user; and

(xxi) any inferences drawn from any of the combined forms of personal data that are used to create a profile of the child user reflecting the child's preferences, choices, characteristics, psychological trends, intelligence, aptitude, and emotional or physical health or behavior.

"Personal data" shall also include any information which creates probabilistic identifiers that can be used to isolate, individualize, or identify a child user or device to a degree of certainty more probable than not based on any item of personal data defined in this paragraph.

(i) "Privacy by default" shall mean that the online product, once released to the public, is predesigned so that the strictest online privacy settings shall apply without any manual input required from the user. In addition, "privacy by default" shall mean that the online product shall only retain personal data provided by a child user for the duration of time necessary to provide such product to such user.

(j) "Process", "processing" or "processor" shall refer to an operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, on behalf of a data controller.

(k) "Sale" or "sold" shall mean the disclosure, dissemination, making available, release, transfer, conveyance, license, rental, or other commercialization of child user data by a data controller to another party, whether commercialization occurs via access to raw data or via use of platform interface. This definition shall include dissemination of child user data, orally, in writing, or by electronic or other means, for monetary or other valuable consideration, or otherwise for a commercial purpose, by a data controller to another party.

(l) "Targeted digital advertising" shall mean an effort to market an online product that is directed at a specific child user or device based on: the personal data of such child user, a group of child users who share personal data identifiers as such term is defined in paragraph (h) of this subdivision, psychological profiling, or a unique identifier of the device; or as a result of such child user or group of child user's use of such online product or any other online product.

(m) "Targeted towards child users" shall mean that the online product should know that its product is accessible to and used by children. The bureau may consider such factors as the online product's internal research about such product's users, existing evidence of user behavior, whether advertisements featured on the online product, including third-party advertisements, are likely to appeal to children, the content of complaints received, as detailed in subparagraph (xiv) of paragraph (a) of subdivision two of this section, about the product from parents, children, or other individuals that indicate the age of users accessing the online product, content and design features of the product such as animation, musical or audio content, the presence of children or influ-

encers popular with children, how the online product describes and promotes itself, and any other characteristic the bureau deems relevant when determining how an online product should know that it is accessible to and used by children.

2. Data protection impact assessments. (a) Each entity offering an online product that is targeted towards child users in this state shall complete a data protection impact assessment. The data protection impact assessment shall include an analysis of the following:

(i) The ways in which child users primarily interact with or consume the online product;

(ii) The amount of time, on average, that a child user spends using the online product and whether the product includes any features that are designed to extend or increase such amount of time;

(iii) The amount and type of data of child users collected, retained, processed, and/or sold;

(iv) The purpose of the collection, retention, processing, or sale of such data;

(v) If the entity is a data controller, the data sharing relationships the entity has with data processors or other third parties with whom it shares the personal data of child users, including any data addendums or other legal policies put into place between the entity and the party receiving the data;

(vi) Data security protections of the online product which work to prevent and respond to data breaches, as defined in subdivision one of this section;

(vii) Any privacy policies, terms of service, or other legal policies published on the online product which relate to child users and whether they are written in a way that can reasonably be understood by a child user;

(viii) Whether such policies or terms of service require approval of the parent or legal guardian of the child user;

(ix) Community standards for published content on the online product, and whether and how the product removes content which violates such standards;

(x) Whether such online product exposes children to potentially harmful content;

(xi) Whether the use of such online product could lead to children being targeted by a potentially harmful contact;

(xii) Whether the online product could allow child users to witness, participate in, or be subject to potentially harmful conduct;

(xiii) Whether the online product shares information on the child user's activity on such product with such child's legal parent or guardian;

(xiv) Opportunities for individuals developing an online product targeted towards child users to voice concerns about such product before, during, and after development without fear of retaliation against such individual;

(xv) Ways in which an entity offering an online product targeted towards child users solicits feedback from children, parents, educators, health professionals, youth development professionals, and the general public on the online product;

(xvi) Whether and how child users can limit exposure to certain types of content;

(xvii) The impact of the online product on a child user's behavioral, emotional, and physical health; and

(xviii) Any other factors the bureau deems relevant to assess the material risk of the online product posed to child users.

(b) Each entity completing such data protection impact assessment shall furnish such assessment to the bureau of internet and technology within five days of receiving a request from the bureau for such assessment. Any potential risks posed by the online product, including risks of noncompliance with any provision of this section or any other law, which are identified by the bureau shall be communicated by the bureau back to the entity, which shall then create a plan to mitigate or eliminate such risk.

(c) The bureau shall provide technical, operational, and legal assistance to entities completing a data protection impact assessment upon the request of the entity. The bureau shall post guidelines for how to complete a data protection impact assessment, including best practices for how to describe data processing, how to ensure data quality and minimization, how to provide privacy information to child users, how to identify and assess risks to child users, how to identify measures to mitigate such risks, and any other practices the bureau deems relevant in its guidance. The bureau shall post such guidelines, along with a model data protection impact assessment template, on a publicly accessible website.

3. Ban on data collection and digital advertising. (a) No entity offering an online product targeted towards child users in this state shall collect, retain, process, or sell the personal data of such users unless such collection, retention, processing, or sale is necessary to provide such online product or to comply with the provisions of this section and such collection, processing, retention, or sale is limited to such purpose. Alternatively, an entity offering an online product may collect, retain, process, or sell the personal data of a child user if it can demonstrate to the bureau that it has a compelling reason to do so which furthers the interest of the child.

(b) No entity offering an online product targeted towards child users in this state shall use targeted digital advertising unless consent for such advertising is obtained from the child's parent or legal guardian and the entity can demonstrate to the bureau that it has a compelling reason to offer such advertising which furthers the interest of the child.

(c) No entity offering an online product targeted towards child users in this state where such product is intended primarily for educational purposes shall collect, retain, process, or sell the personal data of child users.

4. Requirement for certain settings. (a) All entities offering an online product targeted towards child users in this state shall utilize privacy by default, unless the entity can demonstrate a compelling reason to the bureau that an alternative default setting should be used.

(b) All entities offering an online product targeted towards child users must design and activate a feature which proactively alerts child users, in a manner likely to be understood by a child in the age range targeted by the online product, when their personal data is being collected and for the duration of time such collection occurs.

(c) The bureau shall have the discretion to ban auto-play, push notifications, prompts, in-app purchases, or any other feature in an online product targeted towards child users that it deems to be designed to inappropriately amplify the level of engagement a child user has with such product.

5. Deceased child users. All entities offering an online product targeted towards child users in this state shall provide access to such user's account, metadata, and user history to a parent or legal guardian upon the death of such child user and request from such parent or guardian for such access.

6. Law enforcement. All entities offering an online product targeted towards child users in this state shall expedite and prioritize civil and criminal subpoenas and criminal warrants pertaining to child users who have been a victim of a crime with maximum exigence.

7. Terms of service. (a) Any entity offering an online product targeted towards child users in this state shall prominently display a privacy policy and terms of service, to include warnings about potential harms to child users, in a manner which clearly and concisely communicates to a child user, using language likely to be understood by an individual in the age range targeted by such product.

(b) All privacy policies and terms of service of an online product targeted towards child users in this state must be agreed to by both the child user and the parent or legal guardian of such child before such product can become operational for the child user.

(c) Any entity offering an online product targeted towards child users in this state shall clearly post that the terms of service do not impose binding obligations on the child user to the entity.

8. Notification of emergent problems. Any entity offering an online product targeted toward child users in this state shall create and prominently display a method for children, parents, and legal guardians to notify such entity of emergent problems with such product. Such method of notification shall not require the parent, guardian, or child user to have an account on such product in order to notify the entity. All electronic notifications of emergent problems described in this subdivision shall be assigned an identification number and contemporaneously generate an electronic receipt for the notifying individual.

9. Public awareness campaign. Before the effective date of this section and on a regular, ongoing basis, the bureau shall execute a public awareness campaign to inform entities that create digital products targeted towards child users, parents, teachers, and the general public of the provisions of this section in order to ensure maximum compliance thereof. Such campaign may include digital content, billboards, posters, pamphlets, targeted mailers, public service announcements, partnerships with local school districts, or any other method to increase general awareness of the provisions of this section.

10. Annual report. The bureau of internet and technology shall produce and transmit a biennial report to the temporary president of the senate, the speaker of the assembly, and the governor summarizing:

(a) the number of entities completing data protection impact assessments and the results thereof;

(b) the amount and type of child user data being collected, retained, processed, and/or sold by such entities and the purpose thereof;

(c) the volume and nature of material risks posed to child users by such online products and measures taken to mitigate or eliminate such risk;

(d) the volume of notifications of emergent problems and a categorical description of each type of problem (i.e. material that led to child sexual abuse or grooming, instances of suicide or drug overdose related to use of online products by child users, instances of bullying facilitated by online products);

(e) a description of the policies and terms of service being presented to child users and their parents or legal guardians as well as acceptance and denial rates of such policies and terms;

(f) the number of individuals or businesses found to be in noncompliance with this act pursuant to subdivision eleven of this section;

(g) the number of individuals or businesses that have cured violations of this section of their own accord after being issued notice of such violation by the bureau;

(h) the number of actions brought against individuals or businesses pursuant to paragraph (a) of subdivision eleven of this section and the results of such actions;

(i) a summary of the public education efforts undertaken by the bureau on an ongoing basis to alert the public and interested stakeholders of the provisions of this section, pursuant to subdivision nine of this section; and

(j) legislative recommendations for improvements to this or any other statute governing digital actors in this state.

11. Penalties. (a) Whenever the attorney general shall believe from evidence satisfactory to him or her that there is a violation of this section, he or she may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation. Wherever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of up to twenty thousand dollars per instance of violation, provided that the latter amount shall not exceed two hundred fifty million dollars.

(b) The attorney general shall provide written notice to all people or businesses of alleged violations at least ninety days before initiating any action described in paragraph (a) of this subdivision. The person or business shall then have an opportunity to cure any alleged violation of this section within such ninety days. If such alleged violation has been cured, the person or business shall send written notice to the attorney general who shall then retain discretion as to whether or not to pursue an action against such person or business.

(c) The proceeds from penalties collected from violations of this section, pursuant to paragraph (a) of this subdivision, shall be disbursed as follows: (i) twenty percent of such proceeds shall be dedicated to the public awareness campaign described in subdivision nine of this section; and (ii) the remaining eighty percent of such proceeds shall be dedicated to the enforcement of this section by the bureau.

(d) An action may be brought against any person or business who has knowingly or recklessly violated this article if such action is brought on behalf of a child user or by next of kin of a deceased child user alleging harm from such violation. A plaintiff who prevails on a claim alleging a violation of this section is entitled to compensatory, actual, and punitive damages, injunctive relief, reasonable attorneys' fees and costs, and other such remedies as a court may deem appropriate.

§ 5. This act shall take effect on the one hundred eightieth day after it shall have become a law and shall apply to all online products targeted towards child users in this state which are made available to the public on or after such effective date. Effective immediately, the addition, amendment and/or repeal of any rules or regulations necessary for the implementation of this act on its effective date are authorized to be made on or before such effective date.