**South Carolina General Assembly**

125th Session, 2023-2024

**H. 4541**

**STATUS INFORMATION**

General Bill

Sponsors: Reps. Guffey, Pope, Henegan, Chapman, Taylor and Felder

Document Path: LC-0388SA24.docx

Introduced in the House on January 9, 2024

Currently residing in the House

Summary: Child Data Privacy and Protection Act

**HISTORY OF LEGISLATIVE ACTIONS**

 Date Body Action Description with journal page number

 11/16/2023 House Prefiled

 11/16/2023 House Referred to Committee on **Judiciary**

 1/9/2024 House Introduced and read first time (House Journal‑page 76)

 1/9/2024 House Referred to Committee on **Judiciary** (House Journal‑page 76)

 1/10/2024 House Member(s) request name added as sponsor: Felder

View the latest  [legislative information](https://www.scstatehouse.gov/billsearch.php?billnumbers=4541&session=125&summary=B)  at the website

**VERSIONS OF THIS BILL**

[11/16/2023](https://www.scstatehouse.gov/sess125_2023-2024/prever/4541_20231116.docx)

A bill

TO AMEND THE SOUTH CAROLINA CODE OF LAWS BY ENACTING THE “CHILD DATA PRIVACY AND PROTECTION ACT” by adding article 9 to chapter 5, title 39 so AS TO PROVIDE DEFINITIONS, TO PROVIDE FOR CERTAIN DATA PROTECTION IMPACT ASSESSMENTS, TO PROVIDE THAT CERTAIN ENTITIES MAY NOT COLLECT, RETAIN, PROCESS, OR SELL CERTAIN PERSONAL DATA, TO PROVIDE THAT CERTAIN ENTITIES SHALL UTILIZE PRIVACY BY DEFAULT, TO PROVIDE THAT USERS MUST HAVE ACCESS TO THEIR ACCOUNTS, TO PROVIDE THAT CERTAIN CIVIL AND CRIMINAL SUBPOENAS AND WARRANTS MUST BE EXPEDITED, TO PROVIDE THAT PRIVACY POLICIES MUST BE PROMINENTLY DISPLAYED, TO PROVIDE FOR METHODS FOR NOTIFICATIONS, TO PROVIDE FOR A PUBLIC AWARENESS CAMPAIGN, TO REQUIRE A REPORT, AND TO PROVIDE FOR A CAUSE OF ACTION.

Be it enacted by the General Assembly of the State of South Carolina:

SECTION 1. This act may be cited as the “Child Data Privacy and Protection Act”.

SECTION 2. Chapter 5, Title 39 of the S.C. Code is amended by adding:

 Article 9

 Child Data Privacy and Protection

 Section 39‑5‑910. As used in this article:

 (1) “Child” or “children” means a consumer or consumers under eighteen years of age.

 (2) “Child user” means a child accessing an online product with a device.

 (3) “Data breach” means 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.

 (4) “Data controller” or “controller” means 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 item. A data controller is not 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.

 (5) “Data protection impact assessment” means an internal evaluation which the Office of the Attorney General requires entities to carry out in order to evaluate the level of risk associated with the entity’s collection, retention, processing, or sale of child user data.

 (6) “Online product” means an online service, feature, or platform that is accessible to users with a digital device.

 (7) “Personal data” or “personal data identifier” means any computerized information about a child user set forth in this item 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 also means information that identifies, relates to, describes, or is reasonably linked to a particular child user including, but not limited to:

 (a) physical address;

 (b) legal name;

 (c) alias;

 (d) unique personal identifier;

 (e) online identifier;

 (f) Internet protocol address;

 (g) e‑mail address;

 (h) account name;

 (i) social security number;

 (j) place of birth;

 (k) date of birth;

 (l) phone number;

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

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

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

 (p) real‑time geolocation data or stored geolocation history;

 (q) any unique biometric data, body measurement, technical analysis, or measurements collected for the purpose of allowing a child user to authenticate himself on a device, Internet application, or web‑based platform;

 (r) names and identifying information of a child user’s immediate family;

 (s) 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;

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

 (u) 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” also includes 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 item.

 (8) “Privacy by default” means that the online product, once released to the public, is predesigned so that the strictest online privacy settings apply without any manual input required from the user. In addition, “privacy by default” means that the online product only retains personal data provided by a child user for the duration of time necessary to provide the product to the user.

 (9) “Process”, “processing”, or “processor” refers 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.

 (10) “Sale” or “sold” means 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 includes 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.

 (11) “Targeted digital advertising” means an effort to market an online product that is directed at a specific child user or device based on: the personal data of the child user, a group of child users who share personal data identifiers as such term is defined in item (7), psychological profiling, or a unique identifier of the device; or as a result of the child user or group of child user’s use of the online product or any other online product.

 (12) “Targeted towards child users” means that the online product should know that its product is accessible to and used by children. The Office of the Attorney General may consider the factors as the online product’s internal research about the 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 Section 39‑5‑920(A)(14), 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 influencers popular with children, how the online product describes and promotes itself, and any other characteristic the office considers relevant when determining how an online product should know that it is accessible to and used by children.

 Section 39‑5‑920. (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 must include an analysis of the following:

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

 (2) 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 the amount of time;

 (3) the amount and type of data of child users collected, retained, processed, or sold;

 (4) the purpose of the collection, retention, processing, or sale of the data;

 (5) 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;

 (6) data security protections of the online product which work to prevent and respond to data breaches, as defined in Section 39‑5‑910;

 (7) 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;

 (8) whether the policies or terms of service require approval of the parent or legal guardian of the child user;

 (9) community standards for published content on the online product, and whether and how the product removes content which violates the standards;

 (10) whether such online product exposes children to potentially harmful content;

 (11) whether the use of the online product could lead to children being targeted by a potentially harmful contact;

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

 (13) whether the online product shares information on the child user’s activity on the product with the child’s legal parent or guardian;

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

 (15) 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;

 (16) whether and how child users can limit exposure to certain types of content;

 (17) the impact of the online product on a child user’s behavioral, emotional, and physical health; and

 (18) any other factors the Office of the Attorney General considers to be relevant to assess the material risk of the online product posed to child users.

 (B) Each entity completing the data protection impact assessment shall furnish the assessment to the Office of the Attorney General within five days of receiving a request from the office for the assessment. Any potential risks posed by the online product, including risks of noncompliance with any provision of this article or any other law, which are identified by the Office of the Attorney General must be communicated by the office back to the entity, which then shall create a plan to mitigate or eliminate the risk.

 (C) The Office of the Attorney General shall provide technical, operational, and legal assistance to entities completing a data protection impact assessment upon the request of the entity. The Office of the Attorney General 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 office considers to be relevant in its guidance. The office shall post the guidelines, along with a model data protection impact assessment template, on a publicly accessible website.

 Section 39‑5‑930. (A) An entity offering an online product targeted towards child users in this State may not collect, retain, process, or sell the personal data of the users unless the collection, retention, processing, or sale is necessary to provide the online product or to comply with the provisions of this article and the 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 Office of the Attorney General that it has a compelling reason to do so which furthers the interest of the child.

 (B) An entity offering an online product targeted towards child users in this State may not use targeted digital advertising unless consent for the advertising is obtained from the child’s parent or legal guardian and the entity can demonstrate to the Office of the Attorney General that it has a compelling reason to offer the advertising which furthers the interest of the child.

 (C) An entity offering an online product targeted towards child users in this State where the product is intended primarily for educational purposes may not collect, retain, process, or sell the personal data of child users.

 Section 39‑5‑940. (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 Office of the Attorney General 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 the collection occurs.

 (C) The Office of the Attorney General has 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 considers to be designed to inappropriately amplify the level of engagement a child user has with the product.

 Section 39‑5‑950. All entities offering an online product targeted towards child users in this State shall provide access to the user’s account, metadata, and user history to a parent or legal guardian upon the death of a child user and request from the parent or guardian for access.

 Section 39‑5‑960. 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.

 Section 39‑5‑970. (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.

 Section 39‑5‑980. Any entity offering an online product targeted toward child users in this State shall create and display prominently a method for children, parents, and legal guardians to notify an entity of emergent problems with the product. The method of notification may not require the parent, guardian, or child user to have an account on the product in order to notify the entity. All electronic notifications of emergent problems described in this section must be assigned an identification number and contemporaneously generate an electronic receipt for the notifying individual.

 Section 39‑5‑990. The Office of the Attorney General 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 article in order to ensure maximum compliance. The 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 article.

 Section 39‑5‑1000. The Office of the Attorney General shall produce and transmit a biennial report to the President of the Senate, the Speaker of the House of Representatives, and the Governor summarizing:

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

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

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

 (4) the volume of notifications of emergent problems and a categorical description of each type of problem including, but not limited to, material that led to child sexual abuse or grooming, instances of suicide or drug overdose related to use of online products by child users, and instances of bullying facilitated by online products;

 (5) 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 the policies and terms;

 (6) the number of individuals or businesses found to be in noncompliance with this article pursuant to Section 39‑5‑1010;

 (7) the number of individuals or businesses that have cured violations of this article of their own accord after being issued notice of the violation by the Office of the Attorney General;

 (8) the number of actions brought against individuals or businesses pursuant to Section 39‑5‑1010(A) and the results of the actions;

 (9) a summary of the public education efforts undertaken by the Office of the Attorney General on an ongoing basis to alert the public and interested stakeholders of the provisions of this article, pursuant to Section 39‑5‑990; and

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

 Section 39‑5‑1010. (A) Whenever the Attorney General believes from evidence satisfactory to him that there is a violation of this article, he may bring an action on behalf of the people of this State in a court of competent jurisdiction to issue an injunction, to enjoin and restrain the continuation of a violation. Wherever the court shall determine in the 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 for each instance of violation, provided that the latter amount may 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 subsection (A). The person or business then has an opportunity to cure any alleged violation of this article within the ninety days. If the alleged violation has been cured, the person or business shall send written notice to the Attorney General who shall retain discretion as to whether or not to pursue an action against the person or business.

 (C) The proceeds from penalties collected from violations of this article, pursuant to subsection (A), must be disbursed as follows:

 (1) twenty percent of the proceeds must be dedicated to the public awareness campaign described in Section 39‑5‑990; and

 (2) the remaining eighty percent of the proceeds must be dedicated to the enforcement of this article by the Attorney General.

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

SECTION 3. This act takes effect one hundred eighty days after the approval by the Governor.

‑‑‑‑XX‑‑‑‑