THE SENATE
THIRTY-SECOND LEGISLATURE, 2024
STATE OF HAWAII

S.B. NO. 2012

JAN 17 2024

A BILL FOR AN ACT

RELATING TO ONLINE PRIVACY FOR CHILDREN.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

SECTION 1. The Hawaii Revised Statutes is amended by adding a new chapter to be appropriately designated and to read as follows:

"CHAPTER

ONLINE PRIVACY PROTECTION FOR CHILDREN

§ -1 Definitions. As used in this chapter:

"Business" means any entity that offers or provides an online service, product, or feature to the public that is likely to be accessed by children.

"Child" or "children" means a consumer or consumers who are under eighteen years of age.

"Data protection impact assessment" means a systematic survey to assess and mitigate risks that arise from the data management practices of the business to children who are reasonably likely to access the online service, product, or feature at issue that arises from the provision of that online service, product, or feature.

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

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

(1) Is directed to children as defined by the Children's Online Privacy Protection Act (15 U.S.C. section 6501 et. seq.);

(2) Is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children;

(3) Markets or advertises to children;

(4) Is substantially similar or the same as an online service, product, or feature included in paragraph (2);

(5) Has design elements that are known to be of interest to children, including but not limited to games, cartoons, music, and celebrities who appeal to children; or

(6) Has a significant amount of its audience that is determined, based on internal company research, to be children.

"Online service, product, or feature" does not mean any of the following:

(1) A broadband access or broadband service, as defined in section 440J-1;

(2) A telecommunications service, as defined in section 269-1; or

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

"Profiling" means any form of automated processing of personal information that uses personal information to evaluate certain aspects relating to a natural person, including analyzing or predicting aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

§ -2 Data protection impact assessments; requirements. (a) Before July 1, 2026, a business that provides an online service, product, or feature likely to be accessed by children shall complete a data protection impact assessment for any

online service, product, or feature likely to be accessed by children that is offered to the public. This subsection shall not apply to an online service, product, or feature that is not offered to the public on or after July 1, 2026.

(b) Beginning July 1, 2026, before any new online service, product, or feature is offered to the public, a business that provides an online service, product, or feature likely to be accessed by children shall complete a data protection impact assessment for any online service, product, or feature likely to be accessed by children and shall maintain documentation of the data protection impact assessment as long as the online service, product, or feature is likely to be accessed by children. The business shall biennially review all data protection impact assessments.

(c) A data protection impact assessment required by this section shall identify the purpose of the online service, product, or feature; how it uses children's personal information; and the risks of material detriment to children that arise from the data management practices of the business. The data protection impact assessment shall address, to the extent applicable, all of the following:

(1) Whether the design of the online product, service, or feature could harm children, including by exposing children to harmful, or potentially harmful, content on the online product, service, or feature;

(2) Whether the design of the online product, service, or feature could lead to children experiencing or being targeted by harmful, or potentially harmful, contacts on the online product, service, or feature;

(3) Whether the design of the online product, service, or feature could permit children to witness, participate in, or be subject to harmful, or potentially harmful, conduct on the online product, service, or feature;

(4) Whether the design of the online product, service, or feature could allow children to be party to or exploited by a harmful, or potentially harmful, contact on the online product, service, or feature;

(5) Whether algorithms used by the online product, service, or feature could harm children;

(6) Whether targeted advertising systems used by the online product, service, or feature could harm children;

(7) Whether and how the online product, service, or feature uses system design features to increase, sustain, or extend use of the online product, service, or feature by children, including the automatic playing of media, rewards for time spent, and notifications; and

(8) Whether, how, and for what purpose the online product, service, or feature collects or processes sensitive personal information of children.

(d) The business shall document any risk of material detriment to children that arises from the data management practices of the business identified in any data protection impact assessment required by this section and shall create a timed plan to mitigate or eliminate the risk before the online service, product, or feature is available to be accessed by children.

(e) Within three business days of a written request by the department of the attorney general, the business shall provide to the attorney general a list of all data protection impact assessments the business has completed.

(f) For any data protection impact assessment completed pursuant to this section, the business shall make the data impact assessment available, within five business days, to the department of the attorney general pursuant to a written request; provided that, notwithstanding any other law, a data protection impact assessment completed pursuant to this section shall be protected as confidential and shall be exempt from public disclosure; provided further that, to the extent any information contained in a data protection impact assessment disclosed to the attorney general includes information subject to attorney-client privilege or work product protection, disclosure pursuant to this subsection shall not constitute a waiver of that privilege or protection.

(g) A data protection impact assessment conducted by a business for the purpose of compliance with any other law shall be considered to comply with this section if the data protection impact assessment meets the requirements of this chapter. A single data protection impact assessment may contain multiple similar processing operations that present similar risks only if each relevant online service, product, or feature is addressed.

§ -3 **Required actions.** A business that provides an online service, product, or feature likely to be accessed by children shall:

(1) Comply with the requirements of section -2 relating to data protection impact assessments;

(2) Estimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business or apply the privacy and data protections afforded to children to all consumers;

(3) Configure all default privacy settings provided to children by the online service, product, or feature to settings that offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children;

(4) Provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service, product, or feature;

(5) If the online service, product, or feature allows the child's parent, guardian, or any other consumer to monitor the child's online activity or track the child's location, provide an obvious signal to the child when the child is being monitored or tracked;

(6) Enforce published terms, policies, and community standards established by the business, including but not limited to privacy policies and those concerning children; and

(7) Provide prominent, accessible, and responsive tools to help children, or if applicable their parents or guardians, exercise their privacy rights and report concerns.

§ -4 **Prohibited practices.** A business that provides an online service, product, or feature likely to be accessed by children shall not:

(1) Use the personal information of any child in a way that the business knows, or has reason to know, is materially detrimental to the physical health, mental health, or well-being of a child;

(2) Profile a child by default unless both of the following criteria are met:

(A) The business can demonstrate it has appropriate safeguards in place to protect children; and

(B) Either of the following is true:

(i) Profiling is necessary to provide the online service, product, or feature requested and only with respect to the aspects of the online service, product, or feature with which the child is actively and knowingly engaged; or

(ii) The business can demonstrate a compelling reason that profiling is in the best interests of children;

(3) Collect, sell, share, or retain any personal information that is not necessary to provide an online service, product, or feature that is likely to be accessed by children unless:

(A) The business can demonstrate a compelling reason that the collecting selling, sharing, or retaining of the personal information is in the

best interests of children likely to access the online service, product, or feature;

(B) The obligations imposed on the business by this chapter restrict the business's ability to comply with federal, state, or local laws or comply with a court order or subpoena to provide personal information;

(C) The obligations imposed on the business by this chapter restrict the business's ability to comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or county authorities. Law enforcement agencies, including any county police department, the department of law enforcement, or any state or county public body that employs law enforcement officers may direct a business pursuant to a law enforcement agency-approved investigation with an active case number not to delete a consumer's personal information, and upon receipt of that direction, a business shall not delete that personal information for ninety

days in order to allow the law enforcement agency to obtain a court-issued subpoena, order, or warrant to obtain a consumer's personal information. For good cause and only to the extent necessary for investigatory purposes, a law enforcement agency may direct a business not to delete the consumer's personal information for additional ninety-day periods. A business that has received direction from a law enforcement agency not to delete the personal information of a consumer who has requested deletion of the consumer's personal information shall not use the consumer's personal information for any purpose other than retaining the personal information to produce to law enforcement agencies in response to a court-issued subpoena, order, or warrant unless the consumer's deletion request is subject to an exemption from deletion under this chapter;

(D) The obligations imposed on the business by this chapter restrict the business's ability to cooperate with law enforcement agencies

concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or county law; or

(E) The obligations imposed on the business by this chapter restrict the business's ability to cooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury; provided that:

(i) The request is approved by a high-ranking agency officer for emergency access to a consumer's personal information;

(ii) The request is based on the agency's good faith determination that it has a lawful basis to access the personal information on a nonemergency basis; and

(iii) The agency agrees to petition a court for an appropriate order within three days and to

destroy the information if that order is not granted;

(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 business can demonstrate a compelling reason that use of the personal information is in the best interests of children;

(5) Collect, sell, or share any precise geolocation information of children by default unless the collection of that precise geolocation information is strictly necessary for the business to provide the service, product, or feature requested and then only for the limited time that the collection of precise geolocation information is necessary to provide the service, product, or feature;

(6) Collect any precise geolocation information of a child without providing actual notice to the child for the duration of that collection that precise geolocation information is being collected;

(7) Use dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature to forego privacy protections, or to take any action that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or well-being; or

(8) Use any personal information collected to estimate age or age range for any other purpose or retain that personal information longer than necessary to estimate age; provided that age assurance shall be proportionate to the risks and data practice of an online service, product, or feature.

§ -5 **Enforcement.** (a) Any business that violates this chapter shall be subject to an injunction and liable for a civil penalty of not more than $2,500 per affected child for each negligent violation or not more than $7,500 per affected child for each intentional violation, which shall be assessed and recovered only in a civil action brought by the department of the attorney general.

(b) Any penalties, fees, and expenses recovered in an action brought under this chapter shall be deposited to the credit of the general fund.

(c) If a business is in substantial compliance with the requirements of section -2, before initiating an action under this chapter, the attorney general shall provide written notice to the business identifying the specific provisions of this chapter that the attorney general alleges have been or are being violated.

(d) If, within ninety days of the notice required by subsection (c), the business cures any noticed violation and provides the attorney general a written statement that the alleged violations have been cured, and sufficient measures have been taken to prevent future violations, the business shall not be liable for a civil penalty for any violation cured pursuant to this subsection.

§ -6 Applicability of chapter; exemptions. (a) Nothing in this chapter shall be interpreted to serve as the basis for a private right of action under this chapter or any other law.

(b) This chapter shall not apply to:

(1) Protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, title 45 Code of Federal Regulations parts 160 and 164, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5);

(2) A covered entity or business associate of a covered entity governed by the privacy, security, and data breach notification rules issued by the United States Department of Health and Human Services, title 45 Code of Federal Regulations parts 160 and 164, established pursuant to the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act, to the extent that the covered entity or business associate maintains, uses, and discloses patient

information in the same manner as protected health information as described in paragraph (1);

(3) Information that meets the following conditions:

(A) Information that is deidentified in accordance with the requirements for deidentification set forth in title 45 Code of Federal Regulations section 164.514; and

(B) Information that is derived from patient information and that was originally collected, created, transmitted, or maintained by an entity regulated by the Health Insurance Portability and Accountability Act or the Federal Policy for the Protection of Human Subjects, also known as the Common Rule;

provided that information that meets these conditions and is subsequently reidentified shall no longer be eligible for the exemption under this paragraph and shall be subject to applicable federal and state data privacy and security laws, including but not limited to the Health Insurance Portability and Accountability Act and this chapter;

(4) Information that is collected, used, or disclosed in research, as defined in title 45 Code of Federal Regulations section 164.501, including but not limited to a clinical trial, and that is conducted in accordance with applicable ethics, confidentiality, privacy, and security rules of title 45 Code of Federal Regulations part 164; the Federal Policy for the Protection of Human Subjects, also known as the Common Rule; good clinical practice guidelines issued by the International Council for Harmonisation; or human subject protection requirements of the United States Food and Drug Administration."

SECTION 2. (a) There is established the Hawaii children's data protection working group to develop best practices for the implementation of section 1 of this Act.

(b) The working group shall consist of individuals with expertise in at least two of the following areas:

(1) Children's data privacy;

(2) Physical health;

(3) Mental health and well-being;

(4) Computer science; and

(5) Children's rights.

(c) The working group shall select a chair and vice chair from among its members and shall consist of the following ten members:

(1) Two members appointed by the governor;

(2) Two members appointed by the president of the senate;

(3) Two members appointed by the speaker of the house of representatives;

(4) Two members appointed by the office of the attorney general; and

(5) Two members of the information privacy and security council.

(d) The working group shall take input from a broad range of stakeholders, including from academia, consumer advocacy groups, and small, medium, and large businesses affected by data privacy policies and shall address and make recommendations on best practices regarding, at minimum, all of the following:

(1) Identifying online services, products, or features likely to be accessed by children;

(2) Evaluating and prioritizing the best interests of children with respect to their privacy, physical

health, and mental health and well-being and evaluating how those interests may be furthered by the design, development, and implementation of an online service, product, or feature;

(3) Ensuring that age assurance methods used by businesses that provide online services, products, or features likely to be accessed by children are proportionate to the risks that arise from the data management practices of the business, privacy protective, and minimally invasive;

(4) Assessing and mitigating risks to children that arise from the use of an online service, product, or feature; and

(5) Publishing privacy information, policies, and standards in concise, clear language suited for the age of children likely to access an online service, product, or feature.

(e) The working group shall submit a report of its findings and recommendations, including any proposed legislation, to the legislature no later than twenty days prior

to the convening of the regular session of 2025 and every two years thereafter.

(f) The members of the working group shall serve without compensation but shall be reimbursed for expenses, including travel expenses, necessary for the performance of their duties.

(g) The working group shall be dissolved on June 30, 2031.

SECTION 3. This Act shall take effect upon its approval.

INTRODUCED BY: 

S.B. NO. 2012

Report Title:
Department of the Attorney General; Online Privacy Protection for Children; Data Privacy; Data Protection Impact Assessment; Online Services; Hawaii Children's Data Protection Working Group; Report to Legislature

Description:
Requires a business that provides an online service, product, or feature likely to be accessed by children to comply with certain data privacy requirements. Requires a business to complete a data protection impact assessment for any online service, product, or feature likely to be accessed by children and maintain documentation of the assessment as long as the online service, product, or feature is likely to be accessed by children. Requires a business to make a data protection impact assessment available to the Attorney General pursuant to a written request and exempts a data protection impact assessment from public disclosure. Prohibits a business that provides an online service, product, or feature likely to be accessed by children from taking certain proscribed actions. Authorizes the Attorney General to seek an injunction or civil penalty against any business that violates certain provisions. Creates the Hawaii Children's Data Protection Working Group. Requires reports to the Legislature.

The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.