THE SENATE
THIRTY-SECOND LEGISLATURE, 2024
STATE OF HAWAII

S.B. NO. 2309

JAN 19 2024

A BILL FOR AN ACT

RELATING TO ONLINE SAFETY 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

HAWAII AGE-APPROPRIATE DESIGN CODE ACT

§ -1 Short title. This chapter shall be known and may be cited as the Hawaii Age-Appropriate Design Code Act.

§ -2 Legislative findings and declaration. The legislature finds that adults, children, and teens alike are frustrated with the effort and expertise it takes to make online experiences safe for children. As the Internet has become more accessible and attractive to children, the government has created laws to protect children online; however, they are not adequate.

Children should be afforded protections not only by online products and services specifically directed at them but by all online products and services they are likely to access.

Therefore, businesses 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 the online service, product, or feature, and if a conflict arises between commercial interests and the best interests of children, businesses should prioritize the privacy, safety, and well-being of children over commercial interests.

The purpose of this chapter is to:

(1) Establish the Hawaii age-appropriate design code to:

(A) Promote privacy protections for children; and

(B) Ensure that online products, services, or features that are likely to be accessed by children are designed in a manner that recognizes the distinct needs of children at different age ranges; and

(2) Establish a children's data protection working group that shall be administratively attached to the department of the attorney general to assess and develop recommendations on the best practices for the implementation of this Act.

§ -3 **Definitions.** As used in this chapter:

"Biometric information" means an individual's physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity. "Biometric information" includes imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

"Broadband internet access service" means a mass-market retail service by wire or radio provided to customers in the State that provides the capability to transmit data to, and receive data from, all or substantially all internet endpoints, including but not limited to any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up internet access service.

"Child" means a consumer who is under the age of eighteen years.

"Collect" means to buy, rent, gather, obtain, receive, or access any personal information pertaining to a consumer by any means. "Collect" includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

"Common branding" means a shared name, service mark, or trademark that the average consumer would understand to mean that two or more entities are commonly owned.

"Consumer" means a natural person who purchases, attempts to purchase, or is solicited to purchase an online service, product, or feature primarily for personal, family, or household purposes and not for resale or distribution.

"Control" means having:

(A) Ownership of, or the power to vote, more than fifty per cent of the outstanding shares of any class of voting security of a business;

(B) Control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or

(C) The power to exercise a controlling influence over the management of an entity.

"Covered business" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that:

(A) Does business in the State;

(B) Collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information; and

(C) Satisfies one or more of the following:

(i) As of January 1 of the calendar year, had annual gross revenues in excess of $25,000,000 in the preceding calendar year;

(ii) Alone or in combination, annually buys, sells, or shares the personal information of

one hundred thousand or more consumers or households; or

(iii) Derives fifty per cent or more of its annual revenues from selling or sharing consumers' personal information;

(2) Any entity that controls or is controlled by a business that shares common branding and consumers' personal information with the business; or

(3) A joint venture or partnership composed of businesses in which each business has at least a forty per cent interest; provided that the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.

"Data protection impact assessment" means a systematic survey to assess and mitigate risks that arise from the data management practices of the covered 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.

"Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice.

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

"Department" means the department of the attorney general.

"Likely to be accessed by children" means it is reasonable to expect that the online service, product, or feature will be accessed by children because it:

(1) Is directed to children as defined by the Children's Online Privacy Protection Act (15 U.S.C. 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) Contains advertisements marketed to children;

(4) Is substantially similar or the same as an online service, product, or feature subject to 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 number of children as its audience, based on internal company research.

"Online service, product, or feature" does not include:

(1) A broadband internet access service;

(2) A telecommunications service, as defined in title 47 United States Code section 153; or

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

"Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. To the extent it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household, "personal information" includes:

(1) Identifiers such as a real name, alias, postal address, unique personal identifier, online

identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;

(2) Any personal information as defined in section 487D-1, 487N-1, or 487R-1;

(3) Characteristics of protected classifications under state or federal law;

(4) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;

(5) Biometric information;

(6) Internet or other electronic network activity information, including but not limited to browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement;

(7) Geolocation data;

(8) Audio, electronic, visual, thermal, olfactory, or similar information;

(9) Professional or employment-related information;

(10) Personally identifiable information contained in education records, protected pursuant to title 20 United States Code section 1232g and defined in title 34 Code of Federal Regulations section 99.3;

(11) Inferences drawn from any of the information identified in this chapter to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes; and

(12) Sensitive personal information.

"Personal information" does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern, or consumer information that is deidentified or aggregate consumer information.

"Precise geolocation information" means any 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, except as prescribed by rules adopted pursuant to this chapter.

"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.

"Publicly available information" means information:

(1) That is lawfully made available from federal, state, or local government records;

(2) That a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media; or

(3) Made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.

"Publicly available information" does not include biometric information collected by a business about a consumer without the consumer's knowledge.

"Sensitive information" means:

(1) Personal information that reveals:

(A) A consumer's social security, driver's license, state identification card, or passport number;

(B) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;

(C) A consumer's precise geolocation;

(D) A consumer's racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership;

(E) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication; or

(F) A consumer's genetic data;

(2) The processing of biometric information for the purpose of uniquely identifying a consumer;

(3) Personal information collected and analyzed concerning a consumer's health; and

(4) Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

"Sensitive personal information" does not include publicly available information.

§ -4 **Covered business that provides an online service, product, or feature likely to be accessed by children; required actions; prohibited actions.** (a) Beginning July 1, 2025, a covered business that provides an online service, product, or feature likely to be accessed by children shall take all of the following actions:

(1) Before any new online service, product, or feature is offered to the public, 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 for the duration that the online service, product, or feature is likely to be accessed by children and biennially review all data protection impact assessments. The data protection impact assessment shall:

(A) Identify:

(i) The purpose of the online service, product, or feature;

(ii) How the online service, product, or feature uses children's personal information; and

(iii) The risks of material detriment to children that arise from the data management practices of the covered business; and

(B) Address, to the extent applicable:

(i) 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;

(ii) 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;

(iii) 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;

(iv) 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;

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

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

(vii) 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 in use, and notifications; and

(viii) Whether, how, and for what purpose the online product, service, or feature collects

or processes sensitive personal information of children;

(2) Document any risk of material detriment to children that arises from the data management practices of the covered business identified in the data protection impact assessment and create a timed plan to mitigate or eliminate the risk before the online service, product, or feature is accessed by children;

(3) Within three business days of a written request by the attorney general, provide to the attorney general a list of all data protection impact assessments the covered business has completed;

(4) Within five business days of a written request by the attorney general, provide to the attorney general a copy of the data protection impact assessment;

(5) 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 covered business or apply the privacy and data protections afforded to children to all consumers;

(6) 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 covered business can demonstrate a compelling reason that a different setting is in the best interests of children;

(7) 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;

(8) 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;

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

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

(b) Beginning July 1, 2025, no covered business that provides an online service, product, or feature likely to be accessed by children shall:

(1) Use the personal information of any child in a way that the covered 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:

(A) The covered 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 covered 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 with which a child is actively and knowingly engaged unless the covered 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;

(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 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 covered 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 an obvious sign 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 the online service, product, or feature to forego privacy protections, or to take any action that the covered business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or well-being; and

(8) Use any personal information collected to estimate age or age range for any other purpose or retain 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.

(c) Any covered business that provides an online service, product, or feature likely to be accessed by children shall:

(1) Comply or cooperate with all applicable federal, state, and local laws, government authorities, court orders, and subpoenas to provide information;

(2) Cooperate with law enforcement agencies concerning conduct or activity that the covered business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law; and

(3) Cooperate with a law enforcement 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 a consumer accessing, procuring, or searching for services regarding contraception, pregnancy care, or perinatal care, including abortion services, shall not constitute a natural person being at risk or danger of

death or serious physical injury; provided further that:

(A) The request for emergency access to a consumer's personal information is approved by the law enforcement agency's department head;

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

(C) The law enforcement agency agrees to petition a court for an appropriate order within three days and to destroy the information if an order is not granted;

A law enforcement agency may direct a covered business pursuant to a law enforcement agency-approved investigation with an active case number to not delete a consumer's personal information. Upon receipt of direction from a law enforcement agency, a covered business shall not delete the consumer's personal information for ninety days to allow the law enforcement agency to obtain a court-issued subpoena, order, or warrant to obtain the consumer's personal information. For good

cause and only to the extent necessary for investigatory purposes, a law enforcement agency may direct a covered business to not delete the consumer's personal information for an additional ninety-day period. A covered business that has received direction from a law enforcement agency to not 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 it to produce to law enforcement in response to a court-issued subpoena, order, or warrant.

(d) A single data protection impact assessment may contain multiple similar processing operations that present similar risks; provided that each relevant online service, product, or feature is addressed.

§ -5 Completion of data protection impact assessment; applicability. (a) By July 1, 2025, a covered business shall complete a data protection impact assessment for any online service, product, or feature likely to be accessed by children and offered to the public before July 1, 2025.

(b) This section shall not apply to an online service, product, or feature that is not offered to the public on or after July 1, 2025.

§ -6 Penalties; civil action; covered business in substantial compliance. (a) Except as provided in subsection (d), any covered business that violates any provision of this chapter shall be subject to penalties of:

(1) Not more than $2,500 for each affected child for each negligent violation; or

(2) Not more than $7,500 for each affected child for each intentional violation,

which sum shall be collected in a civil action brought by the attorney general on behalf of the State.

(b) Notwithstanding the existence of other remedies at law, the attorney general may apply for a temporary or permanent injunction restraining any covered business from violating or continuing to violate this chapter. The injunction shall be issued without bond.

(c) Any penalties, fees, and expenses recovered in an action brought under this chapter shall be deposited into the

consumer privacy special fund established pursuant to section -8.

(d) If a covered business is in substantial compliance with section -4(a)(1) through (5), the attorney general shall provide the covered business with a written notice before initiating an action under this section, identifying the specific provisions of this chapter that the attorney general alleges have been or are being violated by the covered business. If within ninety days of the written notice issued by the attorney general, the covered business cures any noticed violation and provides the attorney general with a written statement that the alleged violations have been cured, and sufficient measures have been taken to prevent future violations, the covered business shall not be liable for a civil penalty for any violation cured pursuant to this subsection.

(e) Nothing in this chapter shall be construed to serve as the basis for a person aggrieved by a violation of this chapter to file an action in court for civil damages.

§ -7 Data protection impact assessments; confidentiality. (a) Notwithstanding any other law to the contrary, a data protection impact assessment is protected as

confidential information and shall be exempt from public disclosure, including disclosure pursuant to requests made under chapter 92F.

(b) To the extent any information contained in a data protection impact assessment disclosed to the attorney general pursuant to section -4(d) includes information subject to attorney-client privilege or work product protection, disclosure pursuant to this section shall not constitute a waiver of that privilege or protection.

§ -8 Consumer privacy special fund. (a) There is established in the state treasury the consumer privacy special fund into which shall be deposited:

(1) All civil penalties, expenses, and attorney fees collected pursuant to this chapter;

(2) Interest earned on moneys in the fund; and

(3) Appropriations made by the legislature.

(b) The fund shall be administered by the department. Moneys in the fund shall be expended by the department to offset costs incurred by the department to administer this chapter.

§ -9 Application of chapter; exemptions. (a) This chapter shall not apply to:

(1) Protected health information collected by a covered entity or business associate governed by title 45 Code of Federal Regulations parts 160 and 164, containing the privacy, security, and breach notification regulations issued by the United States Department of Health and Human Services;

(2) Covered entities governed by title 45 Code of Federal Regulations parts 160 and 164, to the extent the provider or covered entity maintains patient information in the same manner as protected health information as described in paragraph (1); and

(3) Personal information collected as part of a clinical trial or other biomedical research study subject to, or conducted in accordance with, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration; provided that participants are

informed of any inconsistent use of personal information and provide consent.

(b) As used in this section, "business associate", "covered entity", and "protected health information" have the same meanings as defined in title 45 Code of Federal Regulations section 160.103.

§ -10 Rulemaking. The department may adopt rules pursuant to chapter 91 necessary for the purposes of this chapter.

§ -11 Children's data protection working group; establishment. (a) There is established a children's data protection working group that shall be administratively attached to the department to assess and develop recommendations on the best practices for the implementation of this chapter.

(b) The working group shall accept 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 develop recommendations on best practices regarding, at minimum, 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 covered 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 covered 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;

(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; and

(6) How the working group and the department may leverage the substantial and growing expertise of the office of

enterprise technology services in the long-term development of data privacy policies that affect the privacy, rights, and safety of children online.

(c) The working group shall consist of the following members, or their designatees, who shall satisfy the requirements in paragraph (d):

(1) The attorney general, who shall serve as a co-chair pro tempore of the working group until the members of the working group elect a chair and vice chair of the working group;

(2) The chief information officer, who shall serve as a co-chair pro tempore of the working group until the members of the working group elect a chair and vice chair of the working group;

(3) The director of the office of consumer protection;

(4) Two members to be appointed or invited by the governor;

(5) Two members to be appointed or invited by the president of the senate;

(6) Two members to be appointed or invited by the speaker of the house of representatives; and

(7) Two members to be appointed or invited by the attorney general.

The members of the working group shall elect a chair and vice chair of the working group from amongst themselves to replace the co-chairs pro tempore.

(d) All members of the working group shall:

(1) Be residents of the State; and

(2) Have professional knowledge and experience in at least two of the following areas:

(A) Children's data privacy;

(B) Physical health;

(C) Mental health and well-being;

(D) Computer science; and

(E) Children's rights.

(e) The working group shall report 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 odd-numbered year 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) No member of the working group shall be subject to chapter 84 solely because of the member's participation in the working group.

(h) The working group shall be dissolved on June 30, 2030."

SECTION 2. This Act shall take effect upon its approval.

INTRODUCED BY: 

S.B. NO. 2309

Report Title:
Department of the Attorney General, Hawaii Age-Appropriate Design Code Act; Children's Data Protection Working Group; Consumer Privacy Special Fund; Penalties

Description:
Establishes the Hawaii Age-Appropriate Design Code to promote privacy protections for children and ensure that online products, services, or features that are likely to be accessed by children are designed in a manner that recognizes the distinct needs of children at different age ranges. Establishes a Children's Data Protection Working Group, administratively attached to the Department of the Attorney General, to assess and develop recommendations on the best practices for the implementation of the Hawaii Age-Appropriate Design Code. Establishes the Consumer Privacy Special Fund. Establishes penalties.

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