Assembly Bill No. 2273

CHAPTER 320

An act to add Title 1.81.47 (commencing with Section 1798.99.28) to Part 4 of Division 3 of, and to repeal Section 1798.99.32 of, the Civil Code, relating to consumer privacy.

[Approved by Governor September 15, 2022. Filed with Secretary of State September 15, 2022.]

LEGISLATIVE COUNSEL'S DIGEST

AB 2273, Wicks. The California Age-Appropriate Design Code Act.

(1) Existing law, the California Privacy Rights Act of 2020, approved by the voters as Proposition 24 at the November 3, 2020, statewide general election, establishes the California Privacy Protection Agency. Existing law vests the agency with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018 and requires the agency to be governed by a board. Existing law requires businesses to protect consumer privacy and information, make certain disclosures to consumers regarding a consumer's rights under the act in a specified manner, and disclose to consumers that a consumer has the right to request specific pieces of information, including the categories of information those businesses have collected about that consumer.

Existing law, the Parent's Accountability and Child Protection Act, requires a person or business that conducts business in California and that seeks to sell specified products or services to take reasonable steps to ensure that the purchaser is of legal age at the time of purchase or delivery, including verifying the age of the purchaser. Existing law prohibits a person or business that is required to comply with these provisions from retaining, using, or disclosing any information it receives in an effort to verify age from a purchaser or recipient for any other purpose, except as specified, and subjects a business or person that violates these provisions to a civil penalty.

This bill would enact the California Age-Appropriate Design Code Act, which, commencing July 1, 2024, would, among other things, require a business that provides an online service, product, or feature likely to be accessed by children to comply with specified requirements, including a requirement to configure all default privacy settings offered by the online service, product, or feature to the 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, and to provide 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. The bill would require a business, before any new online services, products, or features are offered to the public, to

complete a Data Protection Impact Assessment, as defined, for any online service, product, or feature likely to be accessed by children and maintain documentation of this assessment as long as the online service, product, or feature is likely to be accessed by children. The bill would require a business to make a Data Protection Impact Assessment available, within 5 business days, to the Attorney General pursuant to a written request and would exempt a Data Protection Impact Assessment from public disclosure, as prescribed. The bill would prohibit a business that provides an online service, product, or feature likely to be accessed by children from taking proscribed action, including, if the end user is a child, using personal information for any reason other than a reason for which the 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.

This bill would create the California Children's Data Protection Working Group to deliver a report to the Legislature regarding best practices for the implementation of these provisions, as specified. The bill would require the members of the working group to have certain expertise, including in the areas of children's data privacy and children's rights. The bill would require the working group to 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 make prescribed recommendations on best practices, including identifying online services, products, or features likely to be accessed by children.

This bill would authorize the Attorney General to seek an injunction or civil penalty against any business that violates its provisions. The bill would hold violators 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. The bill would require any penalties, fees, and expenses recovered in an action brought under the act to be deposited in the Consumer Privacy Fund with the intent that they be used to fully offset costs incurred by the Attorney General in connection with the act.

(2) The California Privacy Rights Act of 2020 authorizes the Legislature to amend the act to further the purposes and intent of the act by a majority vote of both houses of the Legislature, as specified.

This bill would declare that its provisions further the purposes and intent of the California Privacy Rights Act of 2020.

(3) Existing constitutional provisions require that a statute that limits the right of access to the meetings of public bodies or the writings of public officials and agencies be adopted with findings demonstrating the interest protected by the limitation and the need for protecting that interest.

This bill would make legislative findings to that effect.

The people of the State of California do enact as follows:

SECTION 1. (a) The Legislature hereby finds and declares all of the following:

(1) The United Nations Convention on the Rights of the Child recognizes that children need special safeguards and care in all aspects of their lives.

(2) As children spend more of their time interacting with the online world, the impact of the design of online products and services on children's well-being has become a focus of significant concern.

(3) There is bipartisan agreement at the international level, in both the United States and in the State of California, that more needs to be done to create a safer online space for children to learn, explore, and play.

(4) Lawmakers around the globe have taken steps to enhance privacy protections for children on the understanding that, in relation to data protection, greater privacy necessarily means greater security and well-being.

(5) 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. In order to help support the design of online products, services, and features, businesses should take into account the unique needs of different age ranges, including the following developmental stages: 0 to 5 years of age or "preliterate and early literacy"; 6 to 9 years of age or "core primary school years"; 10 to 12 years of age or "transition years"; 13 to 15 years of age or "early teens"; and 16 to 17 years of age or "approaching adulthood."

(6) In 2019, 81 percent of voters said they wanted to prohibit companies from collecting personal information about children without parental consent, and a 2018 poll of Californian parents and teens found that only 36 percent of teenagers and 32 percent of parents say that social networking internet websites do a good job explaining what they do with users' data.

(7) While it is clear that the same data protection regime may not be appropriate for children of all ages, children of all ages should nonetheless be afforded privacy and protection, and online products and services should adopt data protection regimes appropriate for children of the ages likely to access those products and services.

(8) Online services, products, or features that are likely to be accessed by children should offer strong privacy protections by design and by default, including by disabling features that profile children using their previous behavior, browsing history, or assumptions of their similarity to other children, to offer detrimental material.

(9) Ensuring robust privacy protections for children by design is consistent with the intent of the Legislature in passing the California Consumer Privacy Act of 2018, and with the intent of the people of the State of California in passing the California Privacy Rights Act of 2020, which finds and declares that children are particularly vulnerable from a negotiating perspective with respect to their privacy rights.

(10) The California Privacy Protection Agency, created by the California Privacy Rights Act of 2020, has substantial and growing expertise that is integral to the development of privacy policy in California.

(b) Therefore, it is the intent of the Legislature to promote privacy protections for children pursuant to the California Age-Appropriate Design Code Act.

(c) It is the intent of the Legislature that the California Age-Appropriate Design Code promote innovation by businesses whose online products, services, or features are likely to be accessed by children by ensuring that those online products, services, or features are designed in a manner that recognizes the distinct needs of children at different age ranges.

(d) It is the intent of the Legislature that businesses covered by the California Age-Appropriate Design Code may look to guidance and innovation in response to the Age-Appropriate Design Code established in the United Kingdom when developing online services, products, or features likely to be accessed by children.

(e) It is the intent of the Legislature that the California Children's Data Protection Working Group consider the guidance provided by the Information Commissioner's Office in the United Kingdom when developing and reviewing best practices or other recommendations related to the California Age-Appropriate Design Code.

(f) It is the intent of the Legislature that the California Children's Data Protection Working Group and the Department of Justice leverage the substantial and growing expertise of the California Privacy Protection Agency in the implementation of this title.

SEC. 2. Title 1.81.47 (commencing with Section 1798.99.28) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.47. THE CALIFORNIA AGE-APPROPRIATE DESIGN CODE ACT

1798.99.28. This title shall be known, and may be cited, as the California Age-Appropriate Design Code Act.

1798.99.29. The Legislature declares that 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 and makes the following findings:

(a) 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 that online service, product, or feature.

(b) If a conflict arises between commercial interests and the best interests of children, companies should prioritize the privacy, safety, and well-being of children over commercial interests.

1798.99.30. (a) For purposes of this title, the definitions in Section 1798.140 shall apply unless otherwise specified in this title.

(b) For the purposes of this title:

(1) "Child" or "children," unless otherwise specified, means a consumer or consumers who are under 18 years of age.

(2) "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.

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

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

(A) The online service, product, or feature is directed to children as defined by the Children's Online Privacy Protection Act (15 U.S.C. Sec. 6501 et seq.).

(B) The online service, product, or feature is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children.

(C) An online service, product, or feature with advertisements marketed to children.

(D) An online service, product, or feature that is substantially similar or the same as an online service, product, or feature subject to subparagraph (B).

(E) An online service, product, or feature that 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.

(F) A significant amount of the audience of the online service, product, or feature is determined, based on internal company research, to be children.

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

(A) A broadband internet access service, as defined in Section 3100.

(B) A telecommunications service, as defined in Section 153 of Title 47 of the United States Code.

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

(6) "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.

1798.99.31. (a) A business that provides an online service, product, or feature likely to be accessed by children shall take all of the following actions:

(1) (A) Before any new online services, products, or features are 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 this assessment as long as the online service, product, or feature is likely to be accessed by children. A business shall biennially review all Data Protection Impact Assessments.

(B) The Data Protection Impact Assessment required by this paragraph 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:

(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, and notifications.

(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 business identified in the Data Protection Impact Assessment required by paragraph (1) 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 business has completed.

(4) (A) For any Data Protection Impact Assessment completed pursuant to paragraph (1), make the Data Protection Impact Assessment available, within five business days, to the Attorney General pursuant to a written request.

(B) Notwithstanding any other law, a Data Protection Impact Assessment is protected as confidential and shall be exempt from public disclosure, including under the California Public Records Act (Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1 of the Government Code).

(C) 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 paragraph shall not constitute a waiver of that privilege or protection.

(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 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 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 business, including, but not limited to, privacy policies and those concerning children.

(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) A business that provides an online service, product, or feature likely to be accessed by children shall not take any of the following actions:

(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.

(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.

(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 with which a child is actively and knowingly engaged, or as described in paragraphs (1) to (4), inclusive, of subdivision (a) of Section 1798.145, unless 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.

(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 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 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.

(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. Age assurance shall be proportionate to the risks and data practice of an online service, product, or feature.

(c) (1) A Data Protection Impact Assessment conducted by a business for the purpose of compliance with any other law complies with this section if the Data Protection Impact Assessment meets the requirements of this title.

(2) 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.

(d) This section shall become operative on July 1, 2024.

1798.99.32. (a) The California Children's Data Protection Working Group is hereby created to deliver a report to the Legislature, pursuant to subdivision (e), regarding best practices for the implementation of this title.

(b) Working Group members shall consist of Californians 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.

(5) Children's rights.

(c) The working group shall select a chair and a vice chair from among its members and shall consist of the following 10 members:

(1) Two appointees by the Governor.

(2) Two appointees by the President Pro Tempore of the Senate.

(3) Two appointees by the Speaker of the Assembly.

(4) Two appointees by the Attorney General.

(5) Two appointees by the California Privacy Protection Agency.

(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 make recommendations to the Legislature 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.

(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.

(6) How the working group and the Department of Justice may leverage the substantial and growing expertise of the California Privacy Protection Agency in the long-term development of data privacy policies that affect the privacy, rights, and safety of children online.

(e) On or before January 1, 2024, and every two years thereafter, the working group shall submit, pursuant to Section 9795 of the Government Code, a report to the Legislature regarding the recommendations described in subdivision (d).

(f) The members of the working group shall serve without compensation but shall be reimbursed for all necessary expenses actually incurred in the performance of their duties.

(g) This section shall remain in effect until January 1, 2030, and as of that date is repealed.

1798.99.33. (a) A business shall complete a Data Protection Impact Assessment on or before July 1, 2024, for any online service, product, or feature likely to be accessed by children offered to the public before July 1, 2024.

(b) This section does not apply to an online service, product, or feature that is not offered to the public on or after July 1, 2024.

1798.99.35. (a) Any business that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) per affected child for each negligent violation or not more than seven thousand five hundred dollars ($7,500) per affected child for each intentional violation, which shall be assessed and recovered only in a civil action brought in the name of the people of the State of California by the Attorney General.

(b) Any penalties, fees, and expenses recovered in an action brought under this title shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160,

with the intent that they be used to fully offset costs incurred by the Attorney General in connection with this title.

(c) (1) If a business is in substantial compliance with the requirements of paragraphs (1) through (4), inclusive, of subdivision (a) of Section 1798.99.31, the Attorney General shall provide written notice to the business, before initiating an action under this title, identifying the specific provisions of this title that the Attorney General alleges have been or are being violated.

(2) If, within 90 days of the notice required by this subdivision, 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 subdivision.

(d) Nothing in this title shall be interpreted to serve as the basis for a private right of action under this title or any other law.

(e) The Attorney General may solicit broad public participation and adopt regulations to clarify the requirements of this title.

1798.99.40. This title does not apply to the information or entities described in subdivision (c) of Section 1798.145.

SEC. 3. The Legislature finds and declares that this act furthers the purposes and intent of the California Privacy Rights Act of 2020.

SEC. 4. The Legislature finds and declares that Section 2 of this act, which adds Title 1.81.46 (commencing with Section 1798.99.28) to Part 4 of Division 3 of the Civil Code, imposes a limitation on the public's right of access to the meetings of public bodies or the writings of public officials and agencies within the meaning of Section 3 of Article I of the California Constitution. Pursuant to that constitutional provision, the Legislature makes the following findings to demonstrate the interest protected by this limitation and the need for protecting that interest:

The limitation is needed to encourage businesses, by protecting their proprietary interests, to mitigate risks to children online.

O