Date of Hearing: April 19, 2022

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
AB 2273 (Wicks) – As Introduced February 16, 2022

SUBJECT: The California Age-Appropriate Design Code Act

SUMMARY: This bill would establish the California Age-Appropriate Design Code Act which generally would require businesses that create goods, services, or product features (hereinafter "services") likely to be accessed by children to comply with specified standards, including considering the best interests of children likely to access that service when designing, developing, and providing that service. Specifically, **this bill would**:

1) Provide, beginning January 1, 2024, that a business that provides a service likely to be accessed by a child shall comply with all of the following:

    - Consider the best interests of children likely to access that service when designing, developing, and providing that service and, when in conflict with commercial interests, design, develop, and provide that service in the manner that prioritizes the privacy, safety, and well-being of children.

    - Undertake a Data Protection Impact Assessment for any service likely to be accessed by a child and maintain documentation of this assessment as long as the service is likely to be accessed by a child.

    - Establish the age of consumers with a 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.

    - Maintain the highest level of privacy possible for children by default, including, but not limited to, disabling profiling, unless the business can demonstrate a compelling reason that a different default setting is in the best interests of children likely to access that service.

    - 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 service.

    - If the service allows the child's parent, guardian, or any other consumer to monitor the child's online activity or track their location, provide an obvious signal to the child when they are being monitored or tracked.

    - Universally uphold published terms, policies, and community standards established by the business, including, but not limited to, privacy policies and those concerning children.

    - Provide prominent, accessible, and responsive tools to help children exercise their privacy rights and report concerns.

2) Prohibit, beginning January 1, 2024, a business that provides a service likely to be accessed by a child from taking any of the following actions:

   - Using the PI of any child in a way that is demonstrably harmful to the physical health, mental health, or well-being of a child.

   - Collecting and retaining any PI that is not necessary to provide a service with which a child is actively and knowingly engaged.

   - If a business does not have actual knowledge of the age of a consumer, it shall neither collect nor retain any PI that is not necessary to provide a service with which a consumer is actively and knowingly engaged.

   - Using the PI of a child for any reason other than the reason or reasons for which that PI was collected. If the business does not have actual knowledge of the age of the consumer, the business shall not use any PI for any reason other than the reason or reasons for which that PI was collected.

   - Notwithstanding the right to opt-out of the sale of the consumer's PI (if over 16 years of age, and the right to opt-in if the consumer is a minor), disclose the PI of any child unless the business can demonstrate a compelling reason that disclosure of that PI is in the best interests of the child.

   - Collect any precise geolocation information by default, unless the business can demonstrate a compelling reason that doing so would be in the best interests of the child.

   - Collect any precise geolocation information without providing an obvious sign to the consumer for the duration of that collection that precise geolocation information is being collected.

   - Collect any sensitive PI by default, unless the business can demonstrate a compelling reason that the collection of sensitive PI by default is in the best interests of a child.

   - Use dark patterns or other techniques to lead or encourage consumers to provide PI beyond what is necessary to provide that service, to forego privacy protections, or to otherwise take any action that is demonstrably harmful to the consumer's physical health, mental health, or well-being.

3) Require the California Privacy Protection Agency (CPPA) to establish and convene the California Children's Data Protection Taskforce to evaluate best practices for the implementation the AADC, and to provide support to businesses, as specified.

4) Require the taskforce to make recommendations on best practices regarding, but not limited to, all of the following:

   - Identifying services likely to be accessed by children.

- Evaluating and prioritizing the best interests of children with respect to their privacy, health, and well-being, and issuing guidance to businesses on how to incorporate those interests into the design, development, and implementation of a service.

- Determining the level of certainty with which it is necessary to establish the age of a consumer appropriate to the risks that arise from the data management practices of a business.

- Determining whether a reason is sufficiently compelling to warrant practices that are not consistent with the default setting, data collection, and data disclosure practices.

- Assessing and mitigating risks to children that arise from the use of a service, including specific items for the systematic survey necessary to perform a Data Protection Impact Assessment.

- Publishing privacy information, policies, and standards in concise, clear language suited for the age of children likely to access that service.

5) Require, by April 1, 2024, the CPPA, in consultation with the taskforce, to adopt regulations and publish guidelines to effectuate the purposes of the AADC in a manner consistent, and to the extent possible, with international frameworks for the protection of the privacy and well-being of children.

6) Define terms, such as "agency," "dark pattern," "Data Protection Impact Assessment" and "likely to be accessed by a child."

7) Provide Legislative findings and declarations related to the impact of the design of digital products and services on children's well-being and state the intent of the Legislature to promote privacy protections for children pursuant to the California Age-Appropriate Design Code Act.

EXISTING LAW:

1) Provides, under the U.S. Constitution, that "Congress shall make no law . . . abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the government for a redress of grievances." (U.S. Const., 1st Amend., as applied to the states through the 14th Amendment's Due Process Clause; see Gitlow v. New York (1925) 268 U.S. 652.)

2) Requires, pursuant to the federal Children's Online Privacy Protection Act (COPPA), that an operator of an internet website or online service directed to a child, as defined, or an operator of an internet website or online service that has actual knowledge that it is collecting PI (PI) from a child to provide notice of what information is being collected and how that information is being used, and to give the parents of the child the opportunity to refuse to permit the operator's further collection of information from the child. (15 U.S.C. Sec. 6502.)

3) Establishes the California Consumer Privacy Act of 2018 (CCPA) and provides various rights to consumers pursuant to the act. Subject to various general exemptions, a consumer has, among other things:

- The right to know what PI (PI) a business collects about consumers, as specified, including the categories of third parties with whom the business shares PI.

- The right to know what PI a business sells about consumers, as specified, including the categories of PI that the business sold about the consumer and the categories of third parties to whom the PI was sold, by category or categories of PI for each third party to whom the PI was sold.

- The right to access the specific pieces of information a business has collected about the consumer.

- The right to delete information that a business has collected from the consumer.

- The right to opt-out of the sale of the consumer's PI if over 16 years of age, and the right to opt-in if the consumer is a minor (as exercised by the parent if the minor is under 13, or as exercised by the minor if the minor is between ages 13 and 16).

- The right to equal service and price, despite exercising any of these rights. (Civ. Code Sec. 1798.100 et seq.)

4) Among other things, the California Privacy Rights Act (CPRA), enacted by Proposition 24 in 2020, creates a Privacy Protection Agency (CPPA) in California, vested with full administrative power, authority, and jurisdiction to implement and enforce the CCPA. The agency shall be governed by a five-member board, with the chairperson and one member appointed by the Governor, and the three remaining members appointed by the Attorney General, the Senate Rules Committee, and the Speaker of the Assembly. (Civ. Code Sec. 1798.199.10.)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of this bill**: This bill seeks to require that businesses consider the best interests of children when designing services that children are likely to access online. This bill is sponsored by the 5Rights Foundation.

2) **Author's statement**: According to the author:

> The Internet is increasingly shaping how children socialize, consume entertainment, create, and learn. According to data from UNICEF, approximately one in three internet users is a child under 18 years of age. Among parents with children who have access to the internet, there is a concern about what kids are accessing, and the potential harmful effects of the manner in which that access occurs. Data from Parents Together show that 85 percent of parents are concerned with how much time their kids are spending online – time that has increased since the pandemic. The same percentage of parents think that Congress should require protections for kids online, and help to stop sexual predators, place limits on deceptive advertising, and protect children's privacy.

> Data privacy for children is especially important because its misuse can expose children to harmful material, compulsive behavior loops, and other risks. For example, research from the 5Rights Foundation found that, of the top 100 free apps for kids in one of the major app stores, one in three have overt banner ads, including ads that promote adult-appropriate apps requiring a user to watch the full promo before a box could be closed. Additionally, only 36 percent of California teens and 32 percent of California parents say that social networks do a good job explaining what they do with users' data.
>
> While existing federal and state privacy laws offer important protections that guard children's privacy, there is no coherent, comprehensive law that protects children under 18 from goods, services, and products that endanger their welfare. As a result, online goods, services, and products that are likely to be accessed by kids have been loaded with adult design principals that do not factor in the unique needs of young minds, abilities, and sensibilities, nor offer the highest privacy protections by design and by default. As a result, children under 18 face a number of adverse impacts due to their interactions with online world, including bullying, mental health challenges, and addictive behaviors.

3) **Federal and state efforts to protect children online generally permit online platforms to treat all consumers as adults unless there is actual knowledge that a consumer is a child**: The broadcast of children's television programming stations in the United States is regulated by the Federal Communications Commission (FCC), under regulations colloquially referred to as the Children's Television Act. Since 1997, television stations have been required to broadcast at least three hours per week of programs that are specifically designed to meet the educational and informative needs of children aged 16 and younger. There are also regulations on advertising in broadcast and cable television programming targeting children 12 and younger, including limits on ad time, and prohibitions on advertising of products related to the program currently airing.

   As the internet has become more accessible and attractive to children, the government has similarly created protections to protect children online. Enacted in 1998, the federal Child's Online Privacy Protection Act of 1998 (COPPA), requires the Federal Trade Commission (FTC) to issue and enforce a rule (the Rule) concerning children's online privacy. The FTC notes that:

   > The primary goal of COPPA and the Rule is to place parents in control over what information is collected from their young children online. The Rule was designed to protect children under age 13 while accounting for the dynamic nature of the internet. The Rule applies to operators of commercial websites and online services directed to children under 13 that collect, use, or disclose PI from children, and operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing PI from children under 13.[1]

   In an effort to further protect minors online, California subsequently passed SB 568 (Steinberg, Ch. 336, Stats. 2013), known as Privacy Rights for California Minors in the Digital World, which prohibits the operator of an internet website or other online service or mobile application from marketing or advertising a product or service to a minor if the minor

[1] FTC: Frequently Asked Questions about the Children's Online Privacy Protection Rule, http://www.ftc.gov/privacy/coppafaqs.shtm, [as of Apr. 2, 2021].)

cannot legally purchase the product or participate in the service in California, or, compiling PI to market those products or services. This prohibition only applies to an operator that has actual knowledge that a minor is using its online service or whose site or service is directed to minors. That bill also permits a minor to remove content or information posted to a website or service, as specified.

SB 568 was opposed by the Center for Democracy and Technology, who took issue with the bill's limitation that a website must be directed to minors for the provisions of the bill to apply. SB 568, now codified beginning at Business and Professions Code Sec. 22580, provided that a site or service is "directed to minors" if it is "created for the purpose of reaching an audience that is *predominantly* composed of minors, and is not intended for a more general audience comprised of adults." (Emphasis added.) The definition adds that a site or service would not be deemed to be "directed at minors" merely because it contained links to sites or services that were directed to minors.

Further protecting the rights of minors, the Legislature enacted the California Consumer Protection Act of 2018 (CCPA; Chau, Ch. 55, Stats. 2018) which provides various rights to consumers related to the sale of their PI, as defined. Relevant to this bill, the CCPA prohibits any business, as defined, from selling the PI of minors 16 years of age and under, without prior opt-in consent to the sale of the information. For minors between the ages of 13 and 16, the minor can opt-in to the sale of their PI on their own. For minors under 13 years of age, only a parent or guardian may opt-in to the sale of the minor's information. (Civ. Code Sec. 1798.120.)

Notably, the protections for children online largely focus on regulating the collection and sale of children's PI, rather than ensuring that children are protected from manipulative design (dark patterns), adult content, or other potentially harmful design features. In addition, for the most part, the existing laws protecting minors online are only triggered when an online platform has actual knowledge that children are accessing their website. This has incentivized many social media platforms and other online services to ignore the age of their consumers, so that they do not have to adhere to the standards set out in the laws described above.

4) **Recent informational hearing highlighted challenges children and families face online**: On March 29, 2022, this Committee held an informational hearing entitled, *Protecting Kids Online: Challenges & Opportunities in a Digital World.* Testimony from the hearing indicated that adults, children, and teens alike are frustrated with the effort and expertise it takes to make online experiences safe for children. Dr. J. Radesky, a developmental behavioral pediatrician and researcher described how heavily monetized children's digital spaces are, despite children not fully understanding concepts like behavioral advertising, the value of currency, or persuasive nudges. [19] Dr. Radesky testified:

> By tracking young children's mobile devices, my research team realized how much time young children are spending on platforms not initially designed with children in mind, including YouTube. We partnered with Common Sense Media to analyze the content of children's YouTube viewing histories, finding that the majority of videos young children are watching are not educational, are highly commercialized (featuring toys or other branded products), and many have violent and stereotyped content.[20] On some channels we examined, duration of ads exceeded the duration of the video.[21] Although positive

> content exists on YouTube, children appear to be watching what trends; and because algorithms elevate more outrageous and sticky content, content creators produce more such content to get more clicks and engagement.
>
> In mobile apps, my research has focused on where digital design is crossing the line in terms of manipulating children into watching more ads, playing for longer, making more purchases – also known as 'dark patterns'. In the sample of 154 apps we analyzed, 80% contained at least one type of manipulative design – in the form of pressure from trusted characters, navigation constraints, fabricated time pressure, promises of virtual currencies or gameplay objects, or rewards for watching ads (Radesky et al., in press). It appears that adult design norms are being copied and pasted sloppily into children's products, and this is not good design.

In conclusion, Dr. Radesky noted that there are apps that have been designed with children in mind. "These apps don't collect private identifiers, they contain developmentally meaningful content with stoppage cues and nudges to apply their knowledge to social and physical spaces around them, they don't have distracting ads, don't pressure children to make purchases, and give children the autonomy to choose what to do next. They continuously evaluate their products with child-centered standards. We need more companies that show a duty of care that they understand the responsibility inherent in creating the images and stories that children consume."

This bill, modeled after the Age Appropriate Design Code recently enacted in the United Kingdom, seeks to elevate child-centered design in online products and services that are likely to be accessed by children. The bill would additionally require the CPPA to establish a taskforce to evaluate best practices for the implementation of the bill's provisions, and to provide support to businesses.

In support, a large coalition of organizations representing public health, parent, school and youth groups, researchers, and advocacy organizations write:

> Children across the globe are facing an unprecedented mental health crisis. Even before the onset of COVID-19 and subsequent social distancing and isolation, teen suicide was on the rise; in the US the CDC found that between 2007 to 2017 the suicide rate among people aged 10 to 24 increased by 56%. And in the year between spring of 2020 and 2021 emergency room visits for girls ages 12 to 17 increased by 50%.
>
> In 2020, 81% of 14 to 22-year-olds said they used social media either "daily" or "almost constantly." This is by design. As private companies beholden to shareholders, performance incentives for product developers and executives are tied to profit and therefore time spent on their platform. Social media platforms and tech companies do not design these services with their youngest and most vulnerable users in mind.
>
> Ensuring the safety of tech products is long overdue. We have nutrition labels on food packaging, rigorous testing for cribs and car seats, and yet the technology children use daily from the youngest of ages have little to no safeguards.

5) **AB 2273 seeks to shift the paradigm for protecting children online**: This bill would take a different approach to protecting children online than the state and federal laws described in

Comment 3, above, in two distinct ways. First, the bill would require online platforms likely to be accessed by children to turn privacy and safety settings up to a level that is protective of children's mental and physical health and well-being *unless* the online platform can, with an appropriate level of certainty, determine the age of the consumer. In other words, existing law generally permits online platforms to treat all consumers as adults unless there is actual knowledge that the consumer is under 13 years of age. This bill would instead require that websites and other online services likely to be accessed by children offer privacy and safety protections by default, unless there is reasonable certainty that the consumer is an adult. In addition, the bill clearly spells out what baseline protections are required:

- Disabling profiling.

- Prohibiting businesses from collecting or retaining any PI that is not necessary to provide the service requested, or using the PI for any reason other than the reason for which it was collected.

- Prohibiting the collection of any precise geolocation information by default, unless the business can demonstrate a compelling reason that doing so is in the best interest of the child.

- Prohibiting the use of dark patterns (e.g., manipulative design) to lead or encourage consumers to provide PI beyond what is necessary to provide the requested service, or to forgo privacy protections.

In support, Roblox, an online gaming platform, writes that despite the fact that the United Kingdom's AADC is a Code of Practice specific to the UK, Roblox chose to introduce many of its protections globally. Roblox writes:

> We believe that when safety practices faithfully serve the needs of all young people, it makes sense to apply them universally. Consistent with this philosophy, we welcome the introduction of AB 2273 in California, formalizing such protections for California's youth. Specifically, we note the following characteristics of AB 2273:
>
> - It is Principle-Based: Principle-based approaches to safety promote accountability while remaining flexible enough to allow for future innovation and changes in the technology landscape. Further, as a principles-based approach, the Code can be applied to the diversity of services that are offered to children online today, from nascent, start-up technologies to large, global platforms.
>
> - It is Risk-Based: Companies are often best positioned to address vulnerabilities that may exist on their platforms. The risk-based approach that underpins AB 2273 allows for service-specific means to managing potential risks, avoiding the unintended consequences that a "one size fits all" approach can bring to privacy and safety.
>
> - It Emphasizes the "Best Interests of the Child": AB 2273 requires companies to consider the "best interests of the child" in designing and creating tools and features, helping to ensure that children's well-being remains a key part of the design and implementation process.

- It is Modeled After Existing Legislation: Having seen similar measures to AB 2273 thoughtfully introduced and implemented by UK policymakers last year, we believe they can scale effectively for children in California.

Roblox has long met the spirit of AB 2273, assuming a strong duty of care for the people who use our service regardless of age.

Second, the bill requires businesses to anticipate the likely audience of consumers when designing online products and services, and to design those products or services to prevent reasonably predictable harms to that audience. Writing in support, Oakland Privacy notes the innovative approaches Big Tech has implemented to protect children online in response to the AADC in the United Kingdom:

> Today, Big Tech has the ability to implement the requirements of AB 2273 to further protect children's data rights. In response to the recently enacted UK Age Appropriate Design Code, some of the changes Big Tech has implemented include:
>
> - Instagram (Meta) will now prohibit unknown adults to message minors under 18 years old.
> - Instagram (Meta) encourages children to take a break from the app.
> - Google made SafeSearch the default browsing for minors.
> - Google will expand safeguards to prevent age-sensitive ad categories from being shown to teens.
> - Google will block ad targeting based on the age, gender, or interests of minors.
> - Google Play Store prevents viewing and downloading adult-only apps.
> - Youtube (Google) has turned off autoplay.
> - YouTube (Google) videos uploaded by accounts under 18 years old will be set to private by default.
> - Youtube (Google) has bedtime and break reminders turned on by default.
> - TikTok (Musical.ly) set accounts to private by default.
>
> The innovation undertaken by Big Tech in the United Kingdom to comply with that country's AADC are indeed remarkable. In the United States, however, industry argues that concerns over enforcement make similar actions uncertain.

6) **Opposition expresses concern that vague requirements in the bill would make it difficult to determine how to comply**: The California Chamber of Commerce (heretofore, "Chamber") and TechNet write in opposition to AB 2273 and raise a number of concerns related to arguably vague standards in the bill which would create uncertainty with regard to compliance and enforcement. Electronic Frontier Foundation (EFF), who opposes this bill unless amended to address a number of concerns, echoes this sentiment.

TechNet and the Chamber point to two specific concepts in the bill as causing particular concern. First, they take issue with the requirement that a business must take the best interest of children into consideration when developing online services, and with the requirement that in the event of a conflict between commercial interests and the interests of children, companies should prioritize the privacy, safety, and well-being of children. They write, that the concept is "incredibly difficult to interpret. Different companies, even parents in one

household, will have very different interpretations of what is and isn't in the 'best interests' of children."

Indeed, the concept of "best interests" is one that will likely be very fact specific in practice, and as such is difficult to implement for the purposes of statute. It is unclear what level of consideration a business must give to children's best interests, which makes it difficult for businesses to know at which point they have complied with the law, and similarly makes it difficult for a court to know when a business has violated the law. Accordingly, the author has agreed to move the concept of "best interests" to codified findings and declarations in the bill, which should serve the purpose of informing a court as to the spirit and intent of the law when applying its provisions. (This amendment, along with others to which the author has agreed, are found in Comment 9, below.)

Second, TechNet and Chamber are concerned that "AB 2273 would change the threshold from COPPA's 'directed to children' to 'likely to be accessed by children'. [They argue that] this is an over inclusive standard and would capture far more websites and platforms and subject them to this bill's requirements, which as noted are difficult to interpret and implement."

As noted in Comments 3 and 4 above, creating a threshold that is more protective of children than the status quo appears to be precisely the intent of the author and sponsor. Provisions of COPPA, and similar laws have long incentivized online platforms to create websites and services for a "general audience" rather than creating platforms specifically for children, and have further permitted online products and services to intentionally disregard the reasonably predictable ages of consumers.

That being said, there is language in the federal regulations interpreting COPPA that seemingly encompasses the same concept as the author's definition of "likely to access," and should already be familiar to Californian businesses. By way of reference, this bill would define "likely to be accessed by a child" to mean that "it is reasonable to expect, based on the known audience, the nature of the content, the associated marketing, or the online context, that the good, service, or product feature is more likely than not to be accessed by children."

Separate from the "actual knowledge" standard within COPPA that has been exploited by many online business, other federal regulations interpreting COPPA provide, in part, that the concept of "directed to a child" may be analyzed according to the following:

> In determining whether a Web site or online service, or a portion thereof, is directed to children, the Commission will consider its subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the Web site or online service, as well as whether advertising promoting or appearing on the Web site or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience.

Staff notes that, given the overlap between the definition of "likely to be accessed by a child" in this bill and the language from federal regulations above, the author and proponents of

this bill may actually be very close to finding a definition with which businesses know how to comply.

If this Committee were to approve this bill, the author should continue to work with stakeholders and this Committee to ensure that the concept of "likely to be accessed by children" is vetted and developed in a manner that gives businesses more clarity on how to comply with the provisions of this bill.

7) **Opposition raises concerns with age assurance elements of bill**: AB 2273 would require any business that provides an online service likely to be accessed by a child to "establish the age of consumers with a 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." The bill would further provide that if "a business does not have actual knowledge of the age of a consumer, it shall neither collect nor retain any personal information that is not necessary to provide a good, service, or product feature with which a consumer is actively and knowingly engaged."

EFF expresses concern that this provision will drive businesses to employ invasive age assurance practices. In their "oppose unless amended" letter, EFF writes:

> Because AB 2273 applies directions to businesses to apply stronger protections for children, it is likely that this will incentivize them to affirmatively confirm the ages of their customers. Age verification systems are troubling—requiring such systems could hand over significant power, and private data, to third-party identity verification companies like Clear or ID.me. Additionally, such a system would likely lead platforms to set up elaborate age-verification systems for everyone, meaning that all users would have to submit personal data and submit to more corporate surveillance.

Staff notes that age verification is not necessarily the same thing as identity verification, though they can go hand in hand. Further, the age assurance requirement of the bill is designed to be proportionate to the risks that arise from the online service and their data management practices. Thus, platforms that do not collect geolocation data or sensitive PI , for example, would likely need less thorough age verification methods than platforms that collect and/or sell geolocation information by default. However, to further alleviate concerns raised by stakeholders related to reasonable age assurance, the author offers a variety of amendments which do the following:

- Clarify that businesses must establish the age of consumers with a *reasonable* level of certainty appropriate to the risks that arise from the data management practices of the business.
- Prohibit the use of any PI collected for the purpose of establishing age or age range from being used for any other purpose or from being retained longer than necessary to establish age.
- Require the taskforce within the CPPA to make recommendations on best practices regarding (1) ensuring that age verification 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; and (2) best practices for businesses to prove

compliance with the requirement to establish age with a reasonable level of certainty if they are not permitted to retain the PI used to verify age.

8) **Bill is unclear as to enforcement**: This bill would require the CPPA to develop a task force to evaluate best practices for the implementation of the AADC and to provide support to businesses as they seek to comply with the requirements of the bill. AB 2273 would also require the CPPA, in consultation with the taskforce, to adopt regulations and publish guidelines, as specified, by April 1, 2024.

These elements of the bill appear to be designed to ensure that businesses have the support necessary to comply with the requirements of the AADC, but have provided little comfort to industry. As Chamber and TechNet note in their letter of opposition:

> [O]ur companies have a very different relationship with the Information Commissioner's Office (ICO), the regulator that enforces the AADC. The ICO provides extensive guidance on the AADC, explaining the many subjective requirements and providing detailed examples of how it interprets those standards. Companies have the ability to request additional guidance from the ICO, which also gives companies the ability to fix mistakes before fines or penalties are levied.
>
> AB 2273 would import these standards, which read more like industry best practices, directly into California statute. How these standards are enforced is deeply concerning, as California regulators provide less guidance, fewer opportunities to fix mistakes, and take a much more aggressive approach to fines and penalties.

Similarly, EFF is concerned that "because the bill's key concepts will not be more clearly articulated by the taskforce for another two years, we are concerned about the current lack of specificity."

While the bill is indeed silent on how it will be enforced, such an omission is not uncommon in statute and absent any specific language, the bill will be enforceable by the Attorney General (AG) pursuant this State's Unfair Competition Law UCL, which permits the AG to bring actions for injunctive relief. (Bus. & Prof. Code Sec. 17200 et seq.) That is not to say, however, that enforcement pursuant to the UCL is the most appropriate method by which to enforce the AADC.

Accordingly, as this bill moves through the legislative process, the author should consult with stakeholders to determine an enforcement mechanism that would best incentivize compliance with the provisions of the bill, paying special attention to attention to the following factors: 1) the entity charged with enforcement; 2) the penalties, relief, or other sanctions available; 3) any potential limitation of liability for good faith efforts to comply; and 4) the timing of enforcement in relation to any regulations issued by the CPPA.

9) **Amendments accepted by the author address a variety of concerns raised by this Committee and stakeholders**: Seeking to address a number of concerns raised by this Committee and stakeholders, the author has agreed to a significant number of amendments, which are detailed in the mockup below. In general, the amendments would:

- Move the requirement that businesses must consider the best interests of children in the design of their online products to findings and declarations.

- Replace "demonstrably harmful" with "more than a de minimis risk of harm" which is a standard frequently applied by the courts.
- Incorporate definitions from the CCPA and the CPRA to align the application of all three laws.
- Clarify the timing by which a Data Protection Impact Assessment needs to be completed and provided to the CPPA.
- Clarify in a number of places that a business cannot collect or disclose certain PI of a child, unless it is necessary to provide the service or product requested by the child.
- Strike legislative intent language about enacting future legislation related to enforcement.
- Make other clarifying and technical changes to align terms and phrases within the bill to conform, where possible, with well-established statutory language and case law.

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 ~~digital~~ **online** world, the impact of the design of ~~digital~~ **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 ~~digital~~ **online** products and services specifically directed at them, but by all ~~digital~~ **online** products and services they are likely to access.

(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 ~~digital~~ **online** products and services should adopt data protection regimes appropriate for children of the ages likely to access those products and services.

(8) Products and services that are likely to be accessed by children should offer ~~high~~ **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.

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

SEC. 2. Title 1.81.46 (commencing with Section 1798.99.28~~30~~) is added to Part 4 of Division 3 of the Civil Code, immediately following Title 1.81.45, to read:

TITLE 1.81.46. The California Age-Appropriate Design Code Act

1798.99.28. This chapter shall be known and may be cited as the California Age Appropriate Design 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) Companies 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 service, product, or feature.

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

1798.99.30. For the purposes of this title, the following terms apply:

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

(a) "Agency" means the California Privacy Protection Agency, as established by the California Privacy Rights Act of 2020, approved by the voters as Proposition 24 at the November 3, 2020, statewide general election.

(b) "Board" means the agency's board, as established in Section 1798.199.10.

(c) "Child" or "children," unless otherwise specified, mean a consumer or consumers who is under 18 years of age.

~~(d) "Dark pattern" has the same meaning as defined in subdivision (l) of Section 1798.140.~~

(e) "Data Protection Impact Assessment" means a systematic survey to assess and mitigate risks to children who are **reasonably** likely to access the ~~good~~, service, ~~or~~ product**, or** feature at issue that arises from the provision of that ~~good,~~ service, ~~or~~ product**, or** feature in accordance with specifications promulgated by the California Children's Data Protection Taskforce established pursuant to Section 1798.99.32.

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

(f) "Likely to be accessed by a child" means it is reasonable to expect, based on ~~the known audience,~~ the nature of the content, the associated marketing, ~~or~~ the online context, **or academic or internal research,** that the ~~good,~~ service, ~~or~~ product**, or feature** ~~feature is more likely than not to~~ **would** be accessed by children.

~~(g) "Personal information" has the same meaning as defined in subdivision (v) of Section 1798.140.~~

~~(h) "Sensitive personal information" has the same meaning as defined in subdivision (ae) of Section 1798.140.~~

(i) "Taskforce" means the California Children's Data Protection Taskforce as established by Section 1798.99.32.

1798.99.31. (a) A business that provides a**n online** ~~good,~~ service, ~~or~~ product**, or** feature likely to be accessed by a child shall comply with all of the following:

~~(1) Consider the best interests of children likely to access that good, service, or product feature when designing, developing, and providing that good, service, or product feature, and, when in conflict with commercial interests, design, develop, and provide that good, service, or product feature in the manner that prioritizes the privacy, safety, and well-being of children.~~

(2) Undertake a Data Protection Impact Assessment for any ~~good,~~**online** service, ~~or~~ product**, or feature** likely to be accessed by a child and maintain documentation of this assessment as long as the ~~good,~~ **online** service, ~~or~~ product**, or** feature is likely to be accessed by a child. **A report of the assessment must be provided to the Agency within 12 months of the implementation of this Act and reviewed every 24 months or before any new features are offered to the public.**

(3) Establish the age of consumers 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

~~(4) Maintain the highest level of privacy possible for children by default, including, but not limited to, disabling profiling, unless the business can demonstrate a compelling reason that a different default setting is in the best interests of children likely to access that good, service, or product feature.~~

(5) Configure all default privacy settings offered by the online service, product, or feature to the settings that offer a high level of privacy protection offered by the business.

(5) 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 ~~good,~~**online** service, ~~or~~ product**, or** feature.

(6) If the ~~good,~~**online** service, ~~or~~ product**, or** feature allows the child's parent, guardian, or any other consumer to monitor the child's online activity or track their location, provide an obvious signal to the child when they are being monitored or tracked.

(7) ~~Universally uphold~~**Enforce** published terms, policies, and community standards established by the business, including, but not limited to, privacy policies and those concerning children.

(8) Provide prominent, accessible, and responsive tools to help children**, or where applicable their parent or guardian,** exercise their privacy rights and report concerns.

(b) A business that provides a**n online** ~~good,~~ service, ~~or~~ product**, or** feature likely to be accessed by a child shall not take any of the following actions:

~~(1)~~ Use the personal information of any child in a way that ~~is demonstrably harmful~~**the business knows or has reason to know the online service, product, or feature more likely than not causes or contributes to a more than de minimis risk of harm** to the physical health, mental health, or well-being of a child.

(1) Profile a child by default.

(2) Collect, sell, share, or retain any personal information that is not necessary to provide a ~~good~~, service, ~~or~~ product**, or** feature with which a child is actively and knowingly engaged.

(3) If a business does not have actual knowledge of the age of a consumer, it shall ~~neither~~ **not** collect**, share, sell, or**~~nor~~ retain any personal information that is not necessary to provide a ~~good~~, service, ~~or~~ product**, or** feature with which a consumer is actively and knowingly engaged.

(4) Use the personal information of a child for any reason other than the reason or reasons for which that personal information was collected. If the business does not have actual knowledge of the age of the consumer, the business shall not use any personal information for any reason other than the reason or reasons for which that personal information was collected.

(5) Notwithstanding Section 1798.120, ~~disclose~~ **share or sell** the personal information of any child unless ~~the business can demonstrate a compelling reason that disclosure of that personal information is in the best interests of the child.~~**the sharing or selling of that personal information is necessary to provide the online service, product, or feature as permitted by subdivision (a)(1)-(4) of Section 1798.145.**

(6) Collect**, sell, or share** any precise geolocation information **of children** by default, **unless the collection of that precise geolocation information is necessary 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.** ~~unless the business can demonstrate a compelling reason that doing so would be in the best interests of the child.~~

(7) Collect**, sell, or share** any precise geolocation information without providing an obvious sign to the ~~consumer~~ **child** for the duration of that collection that precise geolocation information is being collected.

~~(8) Collect any sensitive personal information by default, unless the business can demonstrate a compelling reason that the collection of sensitive personal information by default is in the best interests of a child.~~

(9) Use dark patterns or other techniques to lead or encourage consumers to provide personal information beyond what is **reasonably expected for the service the child is accessing and** necessary to provide that ~~good~~, service, or product ~~feature~~, to forego privacy protections, or to otherwise take any action that ~~is demonstrably harmful~~**the business knows or has reason to know the online service or product more likely than not causes or contributes to a more than deminimus risk of harm to the child's** ~~to the consumer's~~ physical health, mental health, or well-being.

(10) Use any personal information collected or processed to establish age or age range for any other purpose, or retain that personal information longer than necessary to establish age. Age assurance shall be proportionate to the risks and data practice of a service, product, or feature.

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

1798.99.32. (a) The agency shall establish and convene a taskforce, the California Children's Data Protection Taskforce, to evaluate best practices for the implementation of this title, and to provide support to businesses, with an emphasis on small and medium businesses, to comply with this title.

(b) By April 1, 2023, the board shall appoint members of the taskforce. Taskforce members shall consist of Californians with expertise in the areas of privacy, physical health, mental health, and well-being, technology, and children's rights.

(c) The taskforce shall make recommendations on best practices regarding, but not limited to, all of the following:

(1) Identifying ~~goods,~~ **online** services, ~~and~~ product**s, or** features likely to be accessed by children.

(2) Evaluating and prioritizing the best interests of children with respect to their privacy, health, and well-being, and issuing guidance to businesses on how ~~to incorporate~~ those

interests ~~into~~ **may be furthered by** the design, development, and implementation of a**n online** ~~good~~, service, ~~or~~ product feature.

(3) ~~Determining the level of certainty with which it is necessary to establish the age of a consumer appropriate to the risks that arise from the data management practices of a business.~~**Ensuring that age verification 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) Determining whether a reason is sufficiently compelling to warrant practices that are not consistent with the default setting, data collection, and data disclosure practices prescribed by this title.~~

(5) Assessing and mitigating risks to children that arise from the use of a**n online** ~~good~~, service,~~or~~ product**, or** feature, including specific ~~items for the systematic survey necessary~~**issues businesses must address** to perform a Data Protection Impact Assessment.

(6) Publishing privacy information, policies, and standards in concise, clear language suited for the age of children likely to access that ~~good~~, service, or product ~~feature~~.

(d) By April 1, 2024, the agency, in consultation with the taskforce, shall adopt ~~regulations and publish guidelines~~, as necessary, to effectuate the purposes of this title ~~in a manner consistent, and to the extent possible, with international frameworks for the protection of the privacy and well-being of children~~.

~~1798.99.33. It is the intent of the Legislature to create subsequent legislation to enforce this title.~~

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

10) **Related legislation**: AB 2486 (Gabriel) would establish the Office for the Protection of Children Online within the CPPA. This bill is set to be heard in this Committee on April, 19, 2022.

AB 2408 (Cunningham) would impose on an operator of a social media platform a duty not to addict child users and would prohibit a social media platform from addicting a child user, as specified, to that platform.

11) **Prior legislation**: AB 1545 (Wicks) would have enacted the Kids Internet Design and Safety Act for the purposes of keeping children safe online and would have prohibited a platform from incorporating specified features with respect to content viewable by a child without first obtaining consent from the parent or guardian. This bill was held in the Assembly appropriations Committee.

AB 1138 (Gallagher, 2019) sought to prohibit a person or business that conducts business in California, and that operates a social media website or application, from allowing a person under 16 years of age to create an account with the website or application unless the website or application obtains the consent of the person's parent or guardian before creating the account.

AB 1665 (Chau, 2019) as introduced, would have prohibited a person or business that conducts business in California, that operates an internet website or application that seeks to use a minor's name, picture, or any information about the minor in connection with third party advertising, as specified, from doing so without obtaining prior parental consent.

AB 375 (Chau, Ch. 55, Stats. 2018) enacted the California Consumer Privacy Protection Act (CCPA), which gives consumers certain rights regarding their PI, including: (1) the right to know what PI that is collected and sold about them; (2) the right to request the categories and specific pieces of PI the business collects about them; and (3) the right to opt-out of the sale of their PI, or opt-in in the case of minors under16 years of age.

SB 568 (Steinberg, Ch. 336, Stats. 2013) *See* Comment 3.

REGISTERED SUPPORT / OPPOSITION:

Support

5rights Foundation
Accountable Tech
Alcohol Justice
Avaaz
Bekind. Tech Fund by Globant Ventures
Center for Countering Digital Hate
Center for Digital Democracy
Center for Humane Technology
Children and Screens
Common Sense
Consumer Federation of America
Consumer Federation of California
Do Curious INC.
Eating Disorders Coalition
Epic
Fair Vote
Fairplay
Je Suis Lá
Joan Ganz Cooney Center - Sesame Workshop
Livemore Screensless
Log Off
Lookup
Me2b Alliance
National Hispanic Media Coalition
Neda
Oakland Privacy
Parents Together Action

Protect Young Eyes
Public Health Advocates
Real Facebook Oversight Board
Remind
Reset Tech
Roblox Corporation
Smart Digital Kids
Sum of Us
Tech Oversight Project
The Children's Partnership
The Signals Network
The Social Dilemma
Tiramisu

Opposition

California Chamber of Commerce
Electronic Frontier Foundation (unless amended)
Technet-technology Network

Analysis Prepared by: Nichole Rocha / P. & C.P. / (916) 319-2200