FUTURE OF PRIVACY FORUM

POLICY BRIEF:
An Analysis of the California Age-Appropriate Design Code

By Chloe Altieri, Policy Counsel, and **Bailey Sanchez,** Policy Counsel

OCTOBER 2022

EXECUTIVE SUMMARY

This Policy Brief provides a summary and analysis of key elements of California's Age-Appropriate Design Code Act (California AADC or the Act). Assembly Bill 2273, the California AADC, was introduced by Assemblymembers Buffy Wicks (D) and Jordan Cunningham (R) on February 16, 2022. The California AADC is intended to further the purposes of the California Consumer Privacy Act (CCPA). The bill unanimously passed both houses of the California Legislature, after several amendments, and was signed into law by Governor Newsom on September 15, 2022. The California AADC will go into effect on July 1, 2024.

The California AADC is a first-of-its-kind privacy by design law in the United States and a significant change in the regulation of the technology industry. Modeled after the United Kingdom's Age Appropriate Design Code (UK AADC), under the framework of the UK's General Data Protection Regulation, the California AADC aims to regulate not only how children's data is processed and managed, but more fundamentally, how children experience online products and services. The California AADC is a novel approach to protecting children online and will likely serve as an influential model in future legislation and regulation across the US.

This Policy Brief summarizes and analyzes the key elements of the California AADC:

- **Covered Entities**
- **Age Estimation**
- **Privacy by Design and Default**
- **General Business Obligations**
- **User-Centric Policies**
- **Data Minimization**
- **Data Protection Impact Assessments**
- **Enforcement and Guidance**

CALIFORNIA AGE-APPROPRIATE DESIGN CODE ACT

NOTE: While the California AADC states that it furthers the purpose of the CCPA, the two laws are legally enforceable independently and are codified in separate parts of the California code. Terms of the California AADC may draw definitions from the CCPA, but the overall interaction of the two laws is unclear.

1. Covered Entities and Scope

The California AADC applies to covered businesses that provide online products, services, and features "likely to be accessed by a child." The law incorporates the definition of covered businesses established by the CCPA. "Child" is defined as any consumer under the age of 18. The "likely to be accessed" standard means that it is *reasonable* for a business to expect that the online service, product, or feature (subsequently referred to as "service") would be accessed by children. (Cal. Civ. Code § 1798.99.30(b)(1),(4)). The law includes six factors to consider:

1. The service is directed to children as defined by the Children's Online Privacy Protection Rule (COPPA).
2. The service is "routinely accessed by a significant number of children," as determined by reliable evidence of audience composition.
3. Advertisements are marketed to children.
4. The service is substantially similar to one "routinely accessed by a significant number of children."
5. The service has design elements known to be of interest to children.
6. A "significant amount of the audience," based on internal company research, is determined to be children.

As defined in CCPA, a business is a legal entity operating for profit that collects consumers' personal information, determines processing of consumers' information, does business in California, and meets one or more of the following requirements: (1) Gross annual revenue > $25 million; (2) Receives personal info of 100,000 or more consumers or households; or (3) Derives more than 50% of annual revenues from selling or sharing consumers' information.

Unlike the CCPA, the California AADC creates blanket exclusions for certain categories of businesses, including broadband internet access services, telecommunications services, and businesses for the use or delivery of physical products. (Cal. Civ. Code § 1798.99.30(b)(4),(5)).

- **Scope of coverage goes beyond COPPA:** The California AADC introduces new compliance obligations for U.S. businesses beyond the requirements codified in COPPA, which defines "child" as individuals under 13 years old. Many more businesses will be subject to the California AADC because the Act includes services likely accessed by 13-17 year olds and teenagers often use the same services that adults use online. The factors laid out in the AADC's "likely to be accessed" definition appear to closely track with the factors assessing whether services are covered by COPPA such as actual knowledge of child users, design elements, or subject matter that appeals to children. However, the AADC creates a broader scope of businesses that must comply with the law because it not only includes these similar factors indicating child-directed services, but also includes services that are traditionally considered mixed or general audience services that are "likely to be accessed" by any users under 18.
- **Undefined terms:** Key terms in this provision including "likely," "reasonable," "routinely," and "significant number" are undefined, raising questions about how individuals should understand the protections and how businesses and regulators will interpret and apply the standard.

2. Age Estimation

The California AADC requires that covered businesses providing an online service, product, or feature that is "likely to be accessed by a child" estimate the age of young users with a "reasonable level of certainty appropriate to the risks that arise from the data management practices" or provide strict privacy protections by default to all users. Businesses must balance the certainty of age estimation appropriately to the risks arising from the business's data management practices or alternatively, apply child-appropriate protections for all consumers. Businesses cannot use any personal information collected for age estimation for any other purpose and that data cannot be retained for longer than necessary to estimate age. (Cal. Civ. Code § 1798.99.31(a)(5)).

> **The text of the California AADC contains a section of legislative findings that will be referenced in this brief. The legislative findings are included in the enacted legislation and are used to state the rationale of the legislative body as well as the intent and purpose of the law. While this section is not legally binding, it may inform other branches of government and the enforcement of the law.**

The legislative findings state that businesses should design services based on young users' estimated ages and unique needs. The listed age ranges to consider are 0 to 5 years, 6 to 9 years, 10 to 12 years, 13 to 15 years, and 16 to 17 years.

- **Risk-based approach:** The Act requires businesses to balance age estimation with the risks "that arise from the data management practices" of the business, but it does not clarify what risks should be considered. The Act does not specify whether these are privacy risks to the user, safety risks to the user, cybersecurity risks to the business, etc. Business will likely struggle to identify what risks should be included in these calculations in addition to determining an appropriate balance without additional guidance.
- **Data collection for age estimation:** Accurately estimating the age of users and attempting to identify their appropriate age range may necessitate that companies collect more personal information from users. Determining the age of users may require verification methods such as collecting date of birth, credit card information, or biometric face recognition. The California AADC requires businesses to engage in a balancing test of risk to children's privacy, but the law provides little guidance. This requirement has raised constitutional concerns under the *ACLU v. Reno* case regarding the Communications Decency Act (CDA). The California AADC does not prescribe specific methods or make recommendations on how to comply with this age estimation provision.
- **Age ranges:** Although the legislative findings dictate distinct age ranges, it is unclear how businesses should define what is appropriate for each developmental age.

3. Privacy by Design and Default

For covered entities, the California AADC requires the implementation of new protective measures for young users, including configuring default privacy settings to a "high level of privacy." (Cal. Civ. Code § 1798.99.31(a)(6)). "Default" is defined as a preselected option adopted by the business for the online service, product, or feature. A business can be exempt from this requirement if it can demonstrate a "compelling reason" that a different setting is "in the best interests" of children.

In addition to default settings, the non-binding legislative findings state that covered entities should consider the "best interests of children" when designing their online services, products, and features. (Cal. Civ. Code § 1798.99.29(a)). The legislative findings further recommend that businesses prioritize the "privacy, safety, and well-being of children over commercial interests" if commercial interests conflict with the best interest of children.

» **Default high privacy settings:** The California AADC intends to create a baseline of strong privacy protections through default settings and design. However, in some circumstances it is unclear how a business might assess whether a setting offers a high level of privacy or not.

» **Best interests of children:** The "best interests of children" standard is derived from the "best interest of the child" principle from the UN Convention on the Rights of the Child, which the U.S. has not ratified. This standard may be difficult for U.S. businesses to operationalize because "best interest of the child" is not an established U.S. legal standard outside of the family law context.

4. General Business Obligations

The California AADC imposes new limits on profiling, processing geolocation data, and using manipulative design (or "dark patterns") to influence the behavior of children, in addition to other general obligations.

Prohibition of profiling by default: Covered entities are barred from profiling a child by default unless the business has appropriate safeguards and profiling is either necessary to provide the service, *or* the business can demonstrate that profiling is in the best interests of children. "Profiling" means any form of automated processing of personal information to evaluate aspects relating to a person. This includes practices such as analyzing or predicting a user's health, economic situation, interests, or behavior. (Cal. Civ. Code § 1798.99.31.(b)(2)).

Manipulative Design (or "Dark Patterns"): Businesses are prohibited from using manipulative design techniques to encourage children to provide personal information, beyond reasonable expectations, or to encourage children to take any action that the business knows, or should know, is "materially detrimental" to the child's health or well-being. (Cal. Civ. Code § 1798.99.31(b)(7)).

Geolocation data: Businesses may not collect, share, or sell precise geolocation data by default unless it is necessary for the service and is limited to that necessity. (Cal. Civ. Code § 1798.99.31(b)(5)). Furthermore, businesses are required to provide an "obvious sign to the child" for the duration of the time that geolocation information is being collected. (Cal. Civ. Code § 1798.99.31(b)(6)).

Enforcing Published Terms: The law will require covered entities to enforce "published terms, policies, and community standards" established by the business. This includes all privacy policies, and those concerning children. (Cal. Civ. Code § 1798.99.31(a)(9)).

As defined in CCPA, "dark patterns" are a "user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation."

As defined in CCPA, precise geolocation information is "any data that is derived from a device and that is 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 regulations." (Cal. Civ. Code § 1798.140(w)). This definition is subject to further regulations that may include "if the size defined is not sufficient to protect consumer privacy in sparsely populated areas or when the personal information is used for normal operational purposes, including billing." To date, the California Privacy Protection Agency (CPPA) has not issued any regulations to further define "precise geolocation" under the CCPA.

» **What's not in the California AADC:** While the California AADC includes a number of business obligations and prohibitions to regulate children's online experiences, the Act lacks some common elements of comprehensive U.S. child privacy legislation, such as data security safeguards, notice and consent requirements, or specific restrictions on targeted advertising. Instead, the Act focuses on mitigating a broader category of harms through design obligations.

- **Geolocation signals:** Businesses are required to provide an obvious signal to children in all instances of collecting precise geolocation information for the duration of that collection, even if the collection is necessary for the service. Given the shifting definition of precise geolocation information, this may be a compliance hurdle for businesses. It may also introduce friction in the user experience depending on the frequency of signals for normal operational purposes.
- **"Dark patterns" prohibition:** The Act appears to rely on the CCPA's definition of dark patterns. However, the CCPA's application of dark patterns only pertains to consent, whereas the California AADC expands the dark patterns prohibition to cover *any* action a business knows or should know is materially detrimental to a child's health or well-being and appears to apply to a broader range of user interfaces. "Materially detrimental" is not defined.
- **Uncertainty on enforcing terms:** There may be potential unintended consequences with mandating that platforms enforce their terms of service and community standards and subjecting them to legal liability if they do not. While different in scope, Florida's social media bill contains a provision that requires platforms to enforce community standards; the law is the subject of First Amendment litigation and has been appealed to the Supreme Court. Furthermore, because this AADC provision creates liability for businesses that fail to enforce published community guidelines, it may unintentionally result in businesses implementing fewer or lower community guideline requirements.

5. User-Centric Policies

The California AADC requires businesses to provide privacy information, terms, and community standards concisely and using clear language suited to the age of children likely to access the service. This requirement includes not only privacy policies but also any terms of service or company policies (Cal. Civ. Code § 1798.99.31(a)(7)).

Parent monitoring signals: If the service allows the child's guardian, or any other consumer, to monitor the child's online activity or track their location, the business must provide an obvious signal to the young user as monitoring or tracking is occurring. (Cal. Civ. Code § 1798.99.31(a)(8)).

Tools to exercise privacy rights: The law further commands businesses to provide responsive tools to help children report concerns and exercise their privacy rights. All policies and tools must be prominent and accessible to young users. (Cal. Civ. Code § 1798.99(a)(10)).

- **Multiple signal requirements:** As mentioned above, the California AADC requires signals when geolocation information is being collected. The Act makes no mention of how this may interact with the requirement to provide parent monitoring signals, given there may be instances where both geolocation information is being collected and a parent is monitoring a child's activity or tracking their location.
- **Age-appropriate privacy policies:** The California AADC aims to increase transparency and understanding for young users of business data practices. While these efforts may benefit older minors, such as teens, it is unclear how businesses should make information and tools available in a format suitable for very young children who may not be able to read. There are no clear standards to determine what age-appropriate language or tools are, which may raise compliance questions. Also, the Act requires clarity of language in existing policies, but fails to require businesses to maintain any type of policy. Until best practices are determined, there may be a shift towards businesses providing all privacy notices in language suited to the youngest users out of an abundance of caution.

6. Data Minimization

The California AADC regulates the collecting, selling, sharing, or retaining of personal information of a child and prohibits the use of such data in a way that the business knows, or should know, is "materially detrimental" to the health, physical or mental, or well-being of a child. Businesses may not collect, sell, share, or retain personal information that is not necessary for the service with which a child is "actively and knowingly engaged." Additionally, personal information may not be used for any purpose other than the reason it was collected unless the business has a compelling reason that such practice is in the best interests of children. (Cal. Civ. Code § 1798.99.31(b)(1),(3-4)).

- **Differentiation from COPPA:** COPPA regulates how businesses may collect and use personal information obtained *from* children. The California AADC seems to take a broader approach that may include information not only *from* children, but also *about* children such as metadata or augmented data.
- **What's not in the California AADC:** The Act generally regulates collecting children's personal information, but it does not include any mention or make distinctions between specific types of information typically classified as sensitive data such as biometric information, racial identity, or financial information. Furthermore, the use prohibition is tied to using data in a way that is "materially detrimental" to a child without defining material detriment.

7. Data Protection Impact Assessments

Covered entities will be required to complete a Data Protection Impact Assessment (DPIA) for any online service, product, or feature likely to be accessed by children. A DPIA is a systematic process that assesses the risks of a business' data management practices. After July 1, 2024, the law will require entities to complete DPIAs for any new online service, product, or feature before offering them to the public. (Cal. Civ. Code § 1798.99.33).

Under the California AADC, DPIAs must identify the purpose of the service, how children's personal information is used, and the risks of "material detriment" to young users due to the business' data management practices. The DPIAs must account for risks and design features beyond the scope of data protection, including elements such as:

- the likelihood of harm, or potential harm, caused to children
- the likelihood of exposure to harmful content
- the likelihood of experiencing or being targeted by harmful contacts
- whether the design could permit children to witness, participate in, or be subject to harmful conduct
- whether the design could allow children to be a party to or exploited by a harmful contact
- whether algorithms could harm children
- whether targeted advertising systems could harm children
- whether and how the system design features are used to increase, sustain, or extend the use of the product, including the automatic playing of media, rewards for time spent, and notifications
- whether, how, and for what purpose the service collects and processes sensitive child personal information (Cal. Civ. Code § 1798.99.31(a)(1))

This DPIA requires the business to "create a timed plan to mitigate or eliminate the risk" before children access the service. Additionally, entities would be required to provide the California Attorney General with a list within three days after receipt of a written request containing all the DPIAs the business has completed. Businesses must send requested DPIAs to the California Attorney General within 5 days of written request and the DPIAs will be exempt from public disclosure. (Cal. Civ. Code § 1798.99.31(a)(2-4)).

- **Scope of DPIAs:** Other state privacy laws, such as the CCPA, Colorado Privacy Act, and Virginia Consumer Data Protection Act, will also require DPIAs. However, the DPIA requirement under the California AADC is broader in scope and takes a harm-based approach. DPIAs under the California AADC will include harms that may be experienced through use of an online service, rather than traditional privacy risks.
- **Undefined terms:** The DPIA provision includes distinct considerations for businesses regarding their data management practices. The list of elements to include in the DPIAs offers insight into the evaluation of online services, products, and features capabilities for material detriment to children. Yet, the California AADC does not define "material detriment" or "harm." Businesses are explicitly told what the DPIAs must address, but the statute is unclear regarding how covered entities should define or measure harm or have insight into the likelihood of harm.
- **Number of DPIAs:** Because DPIAs are required for any product, service, or *feature*, businesses may need to do multiple assessments for a single product, and ultimately many businesses may be required to complete numerous DPIAs to account for any feature that is likely to be accessed by a child.

8. Enforcement and Guidance

The Act will authorize the California Attorney General to seek an injunction or civil penalty against any business that violates its provisions. Civil penalties would be capped at $2,500 per affected child for each negligent violation or $7,500 per affected child for each intentional violation. For companies who are in "substantial compliance," the Act provides a 90-day cure period before penalties may be pursued. (Cal. Civ. Code § 1798.99.35). Furthermore, the Attorney General is given broad rulemaking authority to adopt regulations to "clarify the requirements" of the California AADC. (Cal. Civ. Code § 1798.99.35(e)).

California Children's Data Protection Working Group: The California AADC directs the creation of a California Children's Data Protection Working Group (Working Group), which will be tasked with making recommendations and best practices that would assist in identifying services likely to be accessed by children, evaluating the best interests of children, ensuring proper risk balancing for age assurance methods, and publishing policies in age-appropriate language. The Working Group will submit a report to the legislature by January 1, 2024, and every two years after, regarding recommendations and best practices for compliance. (Cal. Civ. Code § 1798.99.32).

- **Future guidance:** Unlike the CCPA, the California AADC does not mandate rulemaking in specific areas which may limit the likelihood of clarity on uncertain compliance requirements. However, because the AADC permits rulemaking by the California Attorney General and the AG is charged with enforcement, there may be an incentive to issue regulations to clarify the law's requirements. Additionally, the creation of the Working Group provides some expectations for more precision of the law's terms.
- **Leveraging the UK's guidance:** The California AADC states that the Working Group should consider the guidance provided by the Information Commissioner's Office (ICO) in the UK. The ICO has published extensive guidance for complying with the UK AADC. Given this recommendation, US-based businesses may choose to look to the ICO's guidance until there is further clarification from the Attorney General and the Working Group.

About FPF //

The Future of Privacy Forum is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies.

Want to talk about privacy legislation? Contact us at info@fpf.org, visit www.fpf.org, or follow us on Twitter: @futureofprivacy.

Did we miss anything? Let us know at info@fpf.org, or email to inquire about becoming involved with FPF. This draft brief should not be used as legal advice.