

Comparison of California Age-Appropriate Design Code Act & Florida “Protection of Children in Online Spaces” Legislation

On May 4, 2023, the Florida legislature passed the Florida Digital Bill of Rights Act ([SB 262](#)), which includes a standalone section focused on child privacy entitled “Protection of Children in Online Spaces” and would take effect on July 1, 2024, if signed by the governor. The provisions in this section appear to be inspired by the Age-Appropriate Design Code legislation that has recently passed in California and is already effective in the United Kingdom while also containing some notable differences. This chart compares and highlights key differences between the Florida and California children’s privacy frameworks.

	CA Age-Appropriate Design Code	FL “Protection of Children in Online Spaces”	Comparison
Scope			
Entities covered by the law	<p>“A business that provides an online service, product, or feature likely to be accessed by children.” (Cal. Civ. Code 1798.99.31(a)).</p> <p>The CCPA defines “business” as a legal entity operating for profit that collects consumers’ personal information, determines the processing of consumers’ information, does business in CA, and meets one or more of the following requirements: (1) Gross revenue of more than \$25 million (2) Receives personal info of 100,000 or more consumers or households (3) Derives more than 50% of annual revenues come from selling or sharing consumers’ information. (Cal. Civ. Code § 1798.140(d)).</p> <p>“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.</p>	<p>“An online platform that provides an online service, product, game, or feature likely to be predominantly accessed by children” (Fla. Stat. § 501.1735(2)).</p> <p>“Online platform” means a social media platform as defined in s. 112.23(1), online game, or online gaming platform. (Fla. Stat. § 501.1735(1)(e)).</p> <p>“Social media platform” means a form of electronic communication through which users create online communities or groups to share information, ideas, personal messages, and other content. (Fla. Stat. § 112.23(1)).</p> <p>“Child” means a consumer or consumers who are under 18 years of age. (Fla. Stat. § 501.1735(1)(a)).</p>	<p>Because FL does not provide a minimum revenue or user threshold, some small businesses that may not meet CCPA’s “business” definition may be in the scope of FL. However, CA applies to <i>all</i> online services likely to be accessed by children, while FL focuses on social media and online gaming.</p> <p>The FL law adds the term “predominantly” to the “likely to be accessed” standard, but does not provide</p>

	<p>(C) The delivery or use of a physical product. (Cal. Civ. Code § 1798.99.30(b)(5)).</p> <p>“Child” means a consumer or consumers who are under 18 years of age. (Cal. Civ. Code § 1798.99.30(b)(2)).</p> <p>“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:</p> <p>(A) The service is directed to children as defined by the Children’s Online Privacy Protection Rule (COPPA).</p> <p>(B) The service is “routinely accessed by a significant number of children,” as determined by reliable evidence of audience composition.</p> <p>(C) Advertisements are marketed to children.</p> <p>(D) The service is substantially similar to one “routinely accessed by a significant number of children.”</p> <p>(E) The service has design elements known to be of interest to children.</p> <p>(F) A “significant amount of the audience,” based on internal company research, is determined to be children. (Cal. Civ. Code § 1798.99.30(b)(4)).</p>		<p>any factors for assessing “likely to be predominantly accessed by children.”</p>
--	--	--	---

Requirements

<p>Prohibition on harmful processing</p>	<p>Prohibition against using “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” (Cal. Civ. Code § 1798.99.31(b)(1)).</p>	<p>Prohibition against processing “the personal information of any child if the online platform has actual knowledge of or willfully disregards that the processing may result in substantial harm or privacy risk to children.” (Fla. Stat. § 501.1735(2)(a)).</p> <p>“Processing” means any operation or set of operations performed on personal information or on</p>	<p>FL provides a narrower knowledge threshold by requiring actual knowledge or willful disregard.</p> <p>“Materially detrimental” is undefined in CA, but</p>
---	---	---	---

		sets of personal information, regardless of whether by automated means. (Fla. Stat. § 501.1735(1)(h)). “Substantial harm or privacy risk to children” includes mental health disorders; addictive behaviors; physical violence, online bullying, and harassment; sexual exploitation; the promotion and marketing of tobacco, gambling, alcohol, or narcotic drugs; and predatory, unfair, or deceptive marketing practices or other financial harms. (Fla. Stat. § 501.1735(1)(l)).	FL defines substantial harm or privacy risk to children.
Profiling	Prohibition against profiling, unless: (A) The business can demonstrate it has appropriate safeguards in place to protect children, and (B) Either of the following is true: (i) Profiling is necessary to provide the online service, product, or feature requested and only with respect to the aspects of the online service, product, or feature with which the child is actively and knowingly engaged. (ii) The business can demonstrate a compelling reason that profiling is in the best interests of children. (Cal. Civ. Code § 1798.99.31(b)(2)). “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)).	Prohibition against profiling, unless: 1. The online platform can demonstrate it has appropriate safeguards in place to protect children. 2.a. Profiling is necessary to provide the online service, product, or feature requested for the aspects of the online service, product, or feature with which the child is actively and knowingly engaged; or b. The online platform can demonstrate a compelling reason that profiling does not pose a substantial harm or privacy risk to children. (Fla. Stat. § 501.1735(2)(b)). “Profile” or “profiling” means any form of automated processing performed on personal information to evaluate, analyze, or predict personal aspects relating to the economic situation, health, personal preferences, interests, reliability, behavior, location, or movements of a child. (Fla. Stat. § 501.1735(1)(i)).	For non-essential profiling, CA requires that businesses be able to demonstrate that profiling is in the best interests of children. In contrast, FL requires a compelling reason that profiling does <i>not</i> pose a substantial harm or privacy risk. “Best interests of children” is undefined in CA, whereas FL defines “substantial harm or privacy risk to children.”
Secondary Use Limitations	A business may not “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 “use personal	An online platform may not “collect, sell, share, or retain any personal information that is not necessary to provide an online service, product” or “use personal information of a child for any reason other than the	CA and FL both create limitations for collecting children’s data to only those purposes for

	<p>information for any reason other than a reason for which that personal information was collected...unless the business can demonstrate a compelling reason this is in the best interests of children." (Cal. Civ. Code § 1798.99.31(b)(3)(4)).</p>	<p>reason for which the personal information was collected...unless the online platform can demonstrate a compelling reason this does not pose a substantial harm or privacy risk to children." (Fla. Stat. § 501.1735(2)(c)(d)).</p>	<p>which the data were originally collected. Similarly to the profiling provisions, CA differs from FL by requiring platforms to have a compelling reason to use the data for a separate purpose. Whereas FL requires platforms to have a compelling reason that using the data for a separate purpose is not posing substantial harm. Inevitably, the CA limitations are stricter by requiring platforms to have compelling motivations and not only a defense for using children's data.</p>
Geolocation	<p>A business shall not: "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."</p>	<p>An online platform may not: "Collect, sell, or share any precise geolocation data of children unless the collection of the precise geolocation data is strictly necessary for the online platform to provide the service, product, or feature requested and then only for the limited time that the collection of the precise geolocation data is necessary to provide the service, product, or feature."</p>	<p>FL does not contain the modifier "by default," though the practical implication of this distinction is unclear.</p>

	<p>“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.”</p> <p>(Cal. Civ. Code § 1798.99.31(b)(5)(6)).</p> <p>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)).</p>	<p>“Collect any precise geolocation data of a child without providing an obvious sign to the child for the duration of the collection that the precise geolocation data is being collected.”</p> <p>(Fla. Stat.§ 501.1735(2)(e)(f)).</p> <p>“Precise geolocation data” means information identified through technology that enables the online platform to collect specific location data which directly identifies the specific location of a child with precision and accuracy within a radius of 1,750 feet. (Fla. Stat.§ 501.1735(1)(g)).</p>	
<p>Dark Patterns</p>	<p>Prohibition on using “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.” (Cal. Civ. Code § 1798.99.31(b)(7)).</p> <p>As defined in CCPA, a “dark pattern” is “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation.” (Cal. Civ. Code §1798.140(l)).</p>	<p>Prohibition on using “dark patterns to lead or encourage children to provide personal information beyond what personal information would otherwise be reasonably expected to be provided for that online service, product, game, or feature; to forego privacy protections; or to take any action that the online platform has actual knowledge of or willfully disregards that may result in substantial harm or privacy risk to children.” (Fla. Stat.§ 501.1735(2)(g)).</p> <p>“Dark pattern” is defined as “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice and includes, but is not limited to, any practice the Federal Trade Commission refers to as a dark pattern.” (Fla. Stat. § 501.1735(2)(g)).</p>	<p>FL uses a similar definition, but goes further by including practices already deemed by the FTC to be dark patterns. This mirrors the Connecticut Data Privacy Act.</p>

<p>Data Privacy Impact Assessment</p>	<p>Create a Data Privacy Impact Assessment (DPIA) for any online service, product, or feature likely to be accessed by a child.</p> <p>DPIAs shall address whether the design could: Harm children; Lead to children experiencing or being targeted by harmful contacts; Permit children to be subject to harmful conduct; Expose children to exploitation by harmful contacts; Harm children with its algorithms; Harm children with its targeted advertising systems; Harm children with incentive or engagement features; Collect sensitive personal information. (Cal. Civ. Code § 1798.99.31. (a)(1)).</p>	<p>N/A</p> <p>However, the FL bill places the burden of proof on companies: “If an online platform processes personal information pursuant to subsection (2), the online platform bears the burden of demonstrating that such processing does not violate subsection (2).” (Fla. Stat. § 501.1735(3)).</p> <p>Note: subsection (2) lists all prohibitions contained within this chart.</p>	<p>FL’s lack of a DPIA requirement is a significant absence as this is a central duty under both the CA and UK AADCs. It is a mechanism for identifying the purpose of the online service, how it uses children’s personal information, and the risks of material detriment to children that may arise prior to launching services. However, companies in the scope of FL may ultimately need to conduct similar assessments to be able to demonstrate that services and features do not cause “substantial risk or privacy risk to children”.</p>
<p>Age Estimation</p>	<p>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 of the business” or afford “high” privacy and data protections to all users. (Cal. Civ. Code § 1798.99.31(a)(5)).</p>	<p>N/A</p>	<p>CA either requires age estimation or the same level of privacy protections must be applied to all consumers. FL does not affirmatively require age</p>

	Prohibits covered businesses from using “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 practices of an online service, product, or feature.” (Cal. Civ. Code § 1798.99.31 (b)(8)).	Prohibits online platforms from using “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 . The age estimate must be proportionate to the risks and data practice of an online service, product, or feature.” (Fla. Stat. § 501.1735(2)(g)).	estimation, though similar to CA, prohibits age estimation information from being used for any other purpose and mandates proportionality.
Transparency	<p>Requirement to 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. (Cal. Civ. Code § 1798.99.31(a)(7)).</p> <p>Requires 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)).</p> <p>Requirement to provide an obvious signal to the child when the child is being monitored or tracked for services that allow a parent to track the child’s activity or location. (Cal. Civ. Code § 1798.99.31(a)(8)).</p>	N/A	Without an equivalent provision, the FL law is less focused on transparency.
Default Settings	Requirement to configure all default privacy settings for children to those 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. (Cal. Civ. Code §1798.99.31(a)(6)).	N/A	Without an equivalent provision, the FL law is less focused on privacy by design.

Tools	Requirement to provide prominent, accessible, and responsive tools to help children or parents exercise their privacy rights and report concerns. (Cal. Civ. Code § 1798.99.31(a)(10)).	N/A	Without FL having an equivalent provision, the CA law focuses more on digital literacy and transparency.
Penalties and Enforcement			
Remedy	<p>The Attorney General may impose an injunction and enforce civil penalties of \$2,500 per affected child for each negligent violation or \$7,500 for each intentional violation.</p> <p>Allows for a discretionary 90-day period to cure an alleged violation and avoid penalty.</p> <p>(Cal. Civ. Code § 1798.99.35 (a)).</p>	<p>Violations are an unfair and deceptive trade practice, and the Attorney General’s office may impose a penalty of up to \$50,000 per violation, or up to \$150,000 if the online platform has actual knowledge that the user is under 18 years of age.</p> <p>Allows for a discretionary 45-day period to cure an alleged violation and avoid penalty.</p> <p>(Fla. Stat. § 501.1735(4)).</p>	<p>FL will collect a flat fee for violations instead of basing the fine on how many children had access. Without any carve-outs for certain types of platforms, this imposes a higher relative burden on smaller businesses.</p> <p>Neither law allows for a private right of action.</p>
Rulemaking Authority	Permissive Attorney General rulemaking authority.	Permissive Attorney General rulemaking authority.	Equivalent standard
Working Group	Creates the Children’s Data Protection Working Group to take input from a broad range of stakeholders and make recommendations to the Legislature on best practices for compliance on topics such as identifying services likely to be accessed by children, evaluating proper risk balancing for age assurance methods, and publishing policies in age-appropriate language. (Cal. Civ. Code § 1798.99.32).	N/A	CA’s working group is tasked with making recommendations on several key provisions of the CA AADC. FL does not provide for a working group.