Comparison of California Age-Appropriate Design Code Act & Connecticut's Online Privacy, Data, and Safety Legislation

On June 2, 2023, the Connecticut legislature passed Connecticut Senate Bill 3 (SB 3), which includes youth privacy protections throughout sections 7-13. The bill makes amendments to the Connecticut Data Privacy Act (CTDPA) with the requirements governing minors' data and accounts taking effect on October 1, 2024, if enacted by Governor Lamont. The provisions in these sections 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 Connecticut and California children's privacy frameworks.

	California Age-Appropriate Design Code (CA AADC)	Connecticut Senate Bill 3 (SB 3) "An Act Concerning Online Privacy, Data, and Safety Protections"	**Comparison**
Scope			
Applicability	"A business that provides an online service, product, or feature likely to be accessed by children." (Cal. Civ. Code 1798.99.31(a)). 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)). "Online service, product, or feature" does not mean	SB 3 applies to each "controller that offers any online service, product, or feature to consumers whom such controller has actual knowledge, or willfully disregards, are minors." (Conn. Gen. Stat. Sec. 42-515 § 9(a)). A "**controller**" is "a person who, alone or jointly with others, determines the purpose and means of processing personal data." (Conn. Gen. Stat. Sec. 42-515 § 1(11)). "Online service, product, or feature" does not include "any: (A) Telecommunications service, as defined in 47 USC 153, as amended from time to time, (B) broadband Internet access service, as defined in 47 CFR 54.400, as amended from time to time, or	SB 3 also uses the CA AADC's "online service, product, or feature" scope but retains the CTDPA's "actual knowledge, or wilfully disregards" standard rather than the CA AADC's "likely to be accessed" standard. Additionally, SB 3 maintains consistency with COPPA by defining a "child" as a consumer under 13. The bill adds the term "minor" for consumers under 18 in contrast with the CA AADC

	any of the following: (A) A broadband internet access service, as defined in Section 3100. (B) A telecommunications service, as defined in Section 153 of Title 47 of the United States Code. (C) The delivery or use of a physical product. (Cal. Civ. Code § 1798.99.30(b)(5)). "**Child**" means a consumer or consumers who are under 18 years of age. (Cal. Civ. Code § 1798.99.30(b)(2)). "**Likely to be accessed by children**" means it is reasonable to expect, based on the following indicators, that the online service, product, or feature would be accessed by children: (A) The service is directed to children as defined by the Children's Online Privacy Protection Rule (COPPA). (B) The service is "routinely accessed by a significant number of children," as determined by reliable evidence of audience composition. (C) Advertisements are marketed to children. (D) The service is substantially similar to one "routinely accessed by a significant number of children." (E) The service has design elements known to be of interest to children. (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)).	(C) delivery or use of a physical product." (Conn. Gen. Stat. Sec. 42-515 § 8(8)). "**Child**" is defined as having "the same meaning as provided in COPPA," which is under 13 years of age. (Conn. Gen. Stat. Sec. 42-515 § 1(6)). "**Minor**" means a consumer who is under 18 years of age. (Conn. Gen. Stat. Sec. 42-515 § 8(7)).	which defines "child" as any consumer under 18. The scope of SB 3 is narrower due to the "actual knowledge" standard.
Requirements			

Age Estimation	Requires that covered businesses providing an online service, product, or feature that is "**likely to be accessed by a child**" to estimate the age of child users with a "**reasonable level of certainty appropriate to the risks that arise from the data management practices of the business**" or afford "high" privacy and data protections to all users. (Cal. Civ. Code § 1798.99.31(a)(5)). 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)).	N/A	The CA AADC requires businesses to estimate the age of child users or to apply the same privacy protections to all users alternatively. SB 3 does not require any form of age estimation or assurance, and controllers are only obligated to comply with the bill when they have actual knowledge (or willfully disregard) that a user is a minor.
Data Minimization	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 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)).	Controllers are **prohibited from processing any minor's personal data or any purpose other than the purpose that the data was collected for**, for longer than reasonably necessary to provide the service, or for the purpose of targeted advertising unless necessary to provide the service. This processing **may occur if the controller obtains the minor's consent or**, if the minor is younger than thirteen years of age, **the consent of such minor's parent** or legal guardian in accordance with COPPA. (Conn. Gen. Stat. Sec. 42-515 § 9(b)). "**Targeted advertising**" means "displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet websites or online applications to	The use of data for a secondary purpose is prohibited by SB 3 and the CA AADC. While the CA AADC does not explicitly prohibit or define targeted advertising, it does require that in completing a DPIA, companies assess the risk of harm to children through targeted advertising systems. SB 3 includes a prohibition of targeted advertising and expands the CTDPA's existing provisions by requiring opt-in consent

		predict such consumer's preferences or interests. "Targeted advertising" does not include (A) advertisements based on activities within a controller's own Internet websites or online applications, (B) advertisements based on the context of a consumer's current search query, visit to an Internet website or online application, (C) advertisements directed to a consumer in response to the consumer's request for information or feedback, or (D) processing personal data solely to measure or report advertising frequency, performance or reach." (Conn. Gen. Stat. Sec. 42-515 § 1(39)).	for secondary data uses.
Data Protection Assessments	Create a **Data Protection Impact Assessment (DPIA)** for any online service, product, or feature likely to be accessed by a child. 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 or to **harmful content**; 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)). Companies that conduct a DPIA shall "**document any risk of material detriment** to children that arises from the data management practices of the business	Controllers are required to conduct and document a **data protection assessment (DPA)** for "each of the controller's processing activities that present a heightened risk of harm to a consumer." (Conn. Gen. Stat. §42-522). Controllers that have actual knowledge or wilfully disregard are minors **"shall conduct a data protection assessment for such online service, product, or feature**: (1) In a manner that is consistent with the requirements established in section 42-522 of the general statutes; and (2) that addresses (A) the purpose of such online service, product or feature, (B) the categories of minors' personal data that such online service, product or feature processes,	While DPAs are an existing obligation under the CTDPAA, SB 3 requires controllers to complete DPAs that specifically consider the purpose, use, and potential risks of processing minors' personal data. The CA AADC contains more specific data uses for businesses to assess, such as data use for algorithms, engagement features, and targeted advertising. Both bills require companies to assess harms but define these harms differently. For example, the CA AADC lists potential

	identified in the Data Protection Impact Assessment . . . **and create a timed plan to mitigate or eliminate the risk** before the online service, product, or feature is accessed by children." (Cal. Civ. Code § 1798.99.31. (a)(2)).	(C) the purposes for which such controller processes minors' personal data with respect to such online service, product, or feature, and (D) any heightened risk of harm to minors that is a reasonably foreseeable result of offering such online service, product, or feature to minors." (Conn. Gen. Stat. Sec. 42-515 § 10(a)). "**Heightened risk of harm to minors**" means processing minors' personal data in a manner that presents any reasonably foreseeable risk of (A) any unfair or deceptive treatment of, or any unlawful disparate impact on, minors, (B) any financial, physical or reputational injury to minors, or (C) any physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of minors if such intrusion would be offensive to a reasonable person. (Conn. Gen. Stat. Sec. 42-515 § 8(5)). Controllers that conduct a data protection assessment **must review the DPA to account for "any material change to the processing operations** of the online service, product or feature that is the subject of such data protection assessment; and maintain documentation concerning such data protection assessment for the longer of (A) the three-year period beginning on the date on which such processing operations cease, or (B) as long as such controller offers such online service, product or feature." (Conn. Gen. Stat. Sec. 42-515 § 10(b)).	harm from contacts, conduct, content, and exploitation, while SB 3 includes deceptive treatment, intrusion upon seclusion, and reputational injury in defining "heightened risk of harm." SB 3 additionally allows controllers to have a "rebuttable presumption" in any enforcement action brought by the State AG if controllers have complied with these DPA requirements.

		If a controller conducts a DPA and determines that the online service, product, or feature "poses a heightened risk of harm to minors, such controller **shall establish and implement a plan to mitigate or eliminate such risk**." (Conn. Gen. Stat. Sec. 42-515 § 10(e)).	
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	While SB 3 contains provisions for similar privacy and digital safety protections, the CA AADC also provides these requirements specifically to relevant default settings. Without an equivalent provision, SB 3 is less focused on privacy by design.
Social Media	N/A	Controllers must **unpublish a minor's social media platform account no later than fifteen business days** after the platform receives a request from a minor or, if the minor is younger than sixteen years of age, from such minor's parent or legal guardian." (Conn. Gen. Stat. Sec. 42-515 § 7(6)). Controllers must **delete a minor's social media platform account no later than forty-five business days** after the platform receives a request from a minor or, if the minor is younger than sixteen years of age, from such minor's parent or legal guardian. Controllers shall also "**cease processing such minor's personal data** except where	SB 3 contains provisions specific to social media platforms to set standards for controllers to unpublish or delete social media accounts as requested by minors or their legal guardians. The CA AADC makes no mention of social media platforms.

		the preservation of such minor's social media platform account or personal data is otherwise permitted or required by applicable law." (Conn. Gen. Stat. Sec. 42-515 § 7(6)). "**Unpublish**" means to remove a social media platform account from public visibility. (Conn. Gen. Stat. Sec. 42-515 § 7(6)). "**Social media platform**" means a "public or semi-public Internet-based service or application" that is "primarily intended to connect and allow users to socially interact" within the service. A social media platform is a service that enables a user to: (I) construct a public or semi-public profile for the purposes of signing into and using such service or application, (II) populate a public list of other users with whom the user shares a social connection within such service or application, and (III) create or post content that is viewable by other users, including, but not limited to, on message boards, in chat rooms, or through a landing page or main feed that presents the user with content generated by other users." (Conn. Gen. Stat. Sec. 42-515 § 7(5)). A social media platform is **not one that exclusively provides direct messaging, "primarily consists of news, sports, entertainment, interactive video games, electronic commerce, or content that is preselected** by the provider or which any chat function is incidental to the provision of the content. (Conn. Gen. Stat. Sec. 42-515 § 7(5)).	

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)).	Social media platforms must **establish and describe in a privacy notice "one or more secure and reliable means for submitting a request"** to have a minor's social media account unpublished or deleted. Conn. Gen. Stat. Sec. 42-515 § 7(a)(3)).	The CA AADC includes requirements to provide tools that increase children's accessibility, digital literacy, and transparency. SB 3 includes much more narrow requirements for only social media platforms and is primarily related only to protecting children from unsolicited messages from adults.
Transparency	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)). Requires covered businesses 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)). Required 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)).	N/A	Without an equivalent provision, SB 3 is less focused on transparency.
Prohibitions			

Dark Patterns	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)). 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)).	Controllers are prohibited from processing any minor's personal data to "use any system design feature to significantly increase, sustain or extend any minor's use." (Conn. Gen. Stat. Sec. 42-515 § 9(b)). Controllers shall not "**provide any consent mechanism that is designed to substantially subvert or impair**, or is manipulated with the effect of substantially subverting or impairing, user autonomy, decision making or choice." (Conn. Gen. Stat. Sec. 42-515 § 9(c)).	The CA AADC prohibits the use of dark patterns to encourage children to provide additional information or to cause any material detriment, but the CA AADC does not define "material detriment." In contrast, SB 3 generally requires controllers to consider protecting children from a defined "heightened risk" while also prohibiting any design features that would subvert user decision-making or is designed to increase or sustain a minor's use of the service. Although the two bills differ in language, they have similar intentions and components. Still, SB 3's mentions of manipulative design are more narrowly limited to consent mechanisms.
Digital Safety	N/A	Controllers **shall not "offer any direct messaging apparatus for use by minors** without providing readily accessible and **easy-to-use safeguards to limit the**	SB 3 contains provisions specific to social media platforms to prohibit

		ability of adults to send unsolicited communications to minors with whom they are not connected." This prohibition exempts services whose predominant function is electronic mail or direct messaging consisting of text, photos, or videos that are only visible to the sender and recipient. (Conn. Gen. Stat. Sec. 42-515 § 9(c)).	controllers from offering direct messaging without providing "readily accessible and easy-to-use safeguards" to limit the ability to receive messages from adults who the minor is not connected with. SB 3 and the CA AADC combine concerns of data privacy with digital safety through obligations to consider potential harms and risks to children. SB 3 takes this one step further by specifically placing protections for direct messaging on social media platforms.
Geolocation	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." "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	Controllers **shall not "collect a minor's precise geolocation data** unless: (A) Such precise geolocation data is reasonably necessary for the controller to provide such online service, product or feature and, if such data is necessary to provide such online service, product or feature, such controller may only collect such data for the time necessary to provide such online service, product, or feature; and (B) the **controller provides to the minor a signal indicating that such controller is collecting such precise geolocation data**, which signal shall be available to such minor for the entire duration of	Both SB 3 and the CA AADC limit the collection of precise geolocation information and include an obligation to provide a signal when that information is collected. The CA AADC differs by specifying that the data collection cannot occur "by default."

	information is being collected." (Cal. Civ. Code § 1798.99.31(b)(5)(6)). 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)).	such collection." Or subject to the consent requirement previously discussed. (Conn. Gen. Stat. Sec. 42-515 § 9(b)). "**Precise geolocation data**" means "information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a **radius of one thousand seven hundred fifty feet**. "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility." (Conn. Gen. Stat. Sec. 42-515 § 1(27)).	
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	Prohibition against processing any minor's personal data **for the purposes of profiling for fully automated decisions that produce "any legal or similarly significant effect** concerning the provision or denial by such controller of any financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunity, health care services or access to essential goods or services" unless necessary to provide the service or subject to the consent requirement previously discussed. (Conn. Gen. Stat. Sec. 42-515 § 9(b)). "**Profiling**" means "any form of automated processing performed on personal data to evaluate, analyze or	Profiling is prohibited under both SB 3 and the CA AADC unless it is necessary for the purpose of providing the online service. CA additionally requires that a business is able to demonstrate that profiling is in the best interest of children, while SB 3 is specific to profiling used for automated decisions.

	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)).	predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements." (Conn. Gen. Stat. Sec. 42-515 § 1(30)).	
Prohibition on harmful processing	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)).	Controllers shall "use reasonable care **to avoid any heightened risk of harm to minors** caused by such online service, product or feature." (Conn. Gen. Stat. Sec. 42-515 § 9(a)). "**Process**" and "**processing**" mean any "operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data." (Conn. Gen. Stat. Sec. 42-515 § 1(28)). "**Heightened risk of harm to minors**" means processing minors' personal data in a manner that presents any reasonably foreseeable risk of (D) any unfair or deceptive treatment of, or any unlawful disparate impact on, minors, (E) any financial, physical or reputational injury to minors, or (F) any physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of minors if such intrusion would be offensive to a reasonable person. (Conn. Gen. Stat. Sec. 42-515 § 8(5)). Controllers are prohibited from these processing activities unless the controller "obtains the minor's	SB 3 requires controllers to use reasonable care to avoid "any heightened risk of harm to minors" caused by the online service. The CA AADC similarly prohibits using children's personal data in a way that may be materially detrimental. However, SB 3 defines the risk of harm, whereas the CA AADC does not define "material detriment." SB 3 extends this requirement by prohibiting specific practices like processing minors' personal data for target advertising or for a reason beyond the original purpose of collection. SB 3 contains similar data minimization principles to the CA AADC, but its specificity in defining

		consent or, if the minor is younger than thirteen years of age, the consent of such minor's parent or legal guardian" in compliance with COPPA's verifiable parental consent requirements. (Conn. Gen. Stat. Sec. 42-515 § 9(b)).	the risk of harm may provide more clarity to controllers in scope.
Penalties and Enforcement			
Remedy	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.** Allows for a discretionary **90-day period to cure** an alleged violation and avoid penalty. (Cal. Civ. Code § 1798.99.35 (a)).	The Attorney General has exclusive authority to enforce violations. From **October 1, 2024, to December 31, 2025**, if the Attorney General (AG), in their discretion, determines that "a controller has violated any provisions of sections 8 to 12" but "may cure such alleged violation," the AG **shall provide a notice of the violation and such provision.** (Conn. Gen. Stat. Sec. 42-515 § 13(b)). A controller may send a notice to the Attorney General, within thirty days of receiving notice of their alleged violation, disclosing that the controller did not commit the violation or had "cured such violation and taken measures that are sufficient to prevent further such violations." (Conn. Gen. Stat. Sec. 42-515 § 13(b)). "Beginning on January 1, 2026, the Attorney General may" **provide a controller an opportunity to cure any alleged violation** within the Attorney General's discretion. In this determination, "the Attorney General may consider: (1) The number of such violations that such controller or processor is alleged to have committed;	SB 3's relevant provisions do not specify a fine or remedy for violations beyond allowing the AG to bring an action. Although both SB 3 and the CA AADC allow for a cure period, the CA AADC allots 90 days, while SB 3 specifies 30 days. SB 3 sets out more defined considerations for the AG to determine the allowance of a cure period. Neither law allows for a private right of action.

		(2) the size and complexity of such controller or processor; (3) the nature and extent of such controller's or processor's processing activities; (4) whether there exists a substantial likelihood that such alleged violation has caused or will cause public injury; (5) the safety of persons or property; (6) whether such alleged violation was likely caused by a human or technical error; and (7) the sensitivity of the data." (Conn. Gen. Stat. Sec. 42-515 § 13(b)).	
Rulemaking Authority	Permissive Attorney General rulemaking authority. (Cal. Civ. Code § 1798.99.35).	N/A	SB 3 does not specify rulemaking.
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 intended to provide recommendations on several key provisions of the CA AADC and to help determine best practices. SB 3 does not provide for a working group.