PRIVACY LAW

CALIFORNIA LAWYERS ASSOCIATION

presents

Inaugural Annual Privacy Summit

Session 6, Track 2

Children, Kids, Minors, Young Adults..

What Are They Called And Why Their Privacy Matters!

MCLE: 1.0 Hours

Friday, February 10, 2023
11:30 a.m. – 12:30 p.m.

Speakers:

Cody Venzke, Senior Counsel, Equity in Civic Technology,
Center for Democracy & Technology
Tyler G. Newby, Partner, Litigation, Fenwick & West
Julie Dawson, Chief Policy & Regulatory Officer, Yoti

Conference Reference Materials

Summary of Major Provisions

	Children's Online Privacy Protection Act (15 U.S.C § 6501 et seq.)	California Privacy Rights Act (Cal. Civil Code § 1798.100 et seq.)	California Age-Appropriate Design Code Act (Cal. Civil Code § 1798.99.28 et seq.)	American Data Privacy and Protection Act (117th, HR 8152)	Kids Online Safety Act (117th, S 3663)	Children and Teens Online Privacy Protection Act (117th, S 1628)
Covered Users [p4]	16 C.F.R. 312.2. A "child" is an individual **under the age of 13**.	1798.120(c). A consumer **under the age of 16**; consumers at least 13 and less than 16 may "affirmatively authorize" the sale or sharing, while parents may do so for consumers under 13.	1798.99.30(b)(1). "Child" is a consumer **under 18 years of age.**	Sec. 2(11). A "covered minor" means an" individual under the age of 17."	Sec. 2(2) "Child" means an "individual who is age 12 or younger." (5) "Minor" means "an individual who is **age 16 or younger**."	Retains COPPA's definition of "child" (under 13). Sec. 3(a)(6). A "minor" is "an individual over the age of 12 and under the age of 17."
Covered Platforms [pp4-5]	16 C.F.R. 312.3. An "operator of a Web site or online service **directed to children**, or any operator that has **actual knowledge** that it is collecting or maintaining personal information from a child" is prohibited from collecting personal information from a child without providing notice and receiving verifiable parental consent.	1798.120(c). A business is prohibited from the sale or sharing of the personal information of a consumer under 16 if it has "**actual knowledge**" of the consumer's age without receiving consent.	1798.99.31(a). Applies to a "business" as defined in the CPRA, that "provides an online service, product, or feature **likely to be accessed by children.**"	Sec. 205(a)-(b). A covered entity is subject to ADPPA's provisions regarding covered minors if it "**has knowledge**" that the individual is a covered minor. Sec. 2(20)(A). "Knowledge" varies depending on if the entity is a "high impact social media company," a "large data holder," or merely a "covered entity."	Sec. 2(3) ''Covered platform'' means a "social media service, social network, video game, messaging application, video streaming service, educational service, or an online platform that connects to the internet and that is used, or is **reasonably likely to be used, by a minor**."	Sec. An operator of an online service is prohibited from collecting personal information from a child or minor if the service is "directed to children or minors or is used or **reasonably likely to be used by children or minors**" prior to obtaining "verifiable consent" from the minor or the parent of a child.
Age Verification or Estimation [p7]	Does not require investigation of ages. 1999 Statement of Basis and Purpose, 64 Fed. Reg. 59888, 59889 (Apr. 21, 2000). 16 C.F.R. 312.2 & FAQs. "Mixed audience" services may implement an age gate.	Cal. AG stated that CCPA does "not require a business to investigate or inquire about age." FSOR, app'x A at 170.	1798.99.31(a)(1)(5). Businesses must "**[e]stimate** the age of child users with a **reasonable level of certainty appropriate to the risks** that arise from the data management practices of the business or apply the privacy and data protections afforded to children to all consumers."	Unclear. Although the "**actual knowledge**" standard applied by the ADPPA to covered entities generally likely does not require age verification, it is not clear how the "willful disregard" and "knew or should have known" standards for large data holders and high-impact social media companies would be interpreted.	Sec. 6(c)(1)(C). Annual report must account for the number of individuals using the covered platform reasonably believed to be minors in the US, disaggregated by the age ranges of 0-5, 6-9, 10-12, 13-16.	Retains provisions in COPPA rule for mixed audience services.

	Children's Online Privacy Protection Act (15 U.S.C § 6501 et seq.)	California Privacy Rights Act (Cal. Civil Code § 1798.100 et seq.)	California Age-Appropriate Design Code Act (Cal. Civil Code § 1798.99.28 et seq.)	American Data Privacy and Protection Act (117th, HR 8152)	Kids Online Safety Act (117th, S 3663)	Children and Teens Online Privacy Protection Act (117th, S 1628)
Privacy and Security Obligations Including Notice [pp8-10]	16 C.F.R. 312.3. Operators of a service directed at children or with actual knowledge it is collecting or maintaining personal information from a child may not collect or maintain personal information from a child. Other data rights, including notice, accessing list of information collected; refusing further collection; requesting deletion; security; and retention limitations.	**Child-specific:** 1798.120(c). Consumers under the age of 16 have the right to opt-in to the sale or sharing of their personal information. Other data rights (not limited to children), including notice of personal information collected and disclosed; use, retention, and sharing limitations; deletion and correction; opting out of sale and sharing; limiting sensitive uses of personal information; and non-discrimination for exercising rights.	1798.99.31(a). Businesses must: (6) "Configure all default privacy settings provided to children . . . to settings that offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children." Other data rights, including notice of privacy information, terms of service, policies, and community standards; enforcement of those terms and policies; and providing "prominent, accessible, and responsive tools" to exercise their privacy rights and report concerns	**Child-specific:** Sec. 205(a). Covered entities may not engage in targeted advertising to any individual with respect to whom the entity "has knowledge" is a "covered minor." Other data rights (not limited to children), including notice of data collected and processing; limitations on collection, processing, and transfer of data; mitigating privacy risks in "design, development, and implementation"; non-retaliation for exercising ADPPA rights; access, correction, deletion, and portability; and civil rights protections.	Sec. 5(a)(1). Covered platforms must provide notice, prior to "registration, use, or purchase" by a minor" of platform's "policies and practices" w/r/t "personal data and safeguards for minors" and accessing safeguards and parental tools	Sec. 3(b)(3)(A). Retains and slightly expands COPPA provisions regarding notice and verifiable consent. Other data rights, including preventing collection of more personal information from a minor or child than "is reasonably required"; security; and erasure of personal information related to minors and children.
Duty of Care Obligations (e.g., a free standing design duty) [pp10-11]	n/a	1798.185(a)(15). Businesses must file a risk assessment with the California Privacy Protection Agency.	Cal. AADC Act omits the UK version's obligation to act in the "best interests of the child," but requires businesses to conduct a "Data Protection Impact Assessment" to "assess and mitigate risks that arise from the data management practices of the business," including exposure to "harmful" content, contacts, and conduct.	C**hild-specific:** Sec. 103(a)(b). Covered entities must establish "reasonable policies, practices, and procedures" to "identify, assess, and mitigate privacy risks related to covered minors . . . to result in reasonably necessary and proportionate residual risk to covered minors" in "a manner that considers the developmental needs of different age ranges of covered minors."	Sec. 3(a). "A covered platform shall act in the best interests of a minor that uses the platform's products or services, as described in subsection (b)." Must prevent or mitigate harms related to mental health disorders, self-harm, suicide, eating disorders, and substance use; addiction-like behaviors; physical harm, online bullying, and harassment; sexual exploitation; and promotion and marketing of narcotic drugs, tobacco products, gambling, or alcohol	n/a

	Children's Online Privacy Protection Act (15 U.S.C § 6501 et seq.)	California Privacy Rights Act (Cal. Civil Code § 1798.100 et seq.)	California Age-Appropriate Design Code Act (Cal. Civil Code § 1798.99.28 et seq.)	American Data Privacy and Protection Act (117th, HR 8152)	Kids Online Safety Act (117th, S 3663)	Children and Teens Online Privacy Protection Act (117th, S 1628)
Role of Consent [pp11-12]	16 C.F.R. 312.5(a), (c) and FAQs. "Verifiable parental consent" must be obtained through one of eight approved methods, including use of a credit card or checking a government-issued ID.	1798.120(d). A minor at least 13 and under 16 or parents of a consumer less than 13 may opt in. Cal. Code Regs., tit. 11, § 7070. Parental consent must be obtained through one of six methods.	No consent provisions.	**Child-specific:** Sec. 205(b). Consent must be provided to transfer a covered minor's covered data.	Limited consent provisions, regarding market- and product-focused research on minors.	Sec. 3(a)(4). Retains COPPA's statutory definition of verifiable consent.
Parental Supervision Tools [pp12-14]	16 C.F.R. 312.4(a)-(c). Must provide direct notice to a parent prior to collecting or maintaining personal information from a child. 16 C.F.R. 312.6(a). Must provide parents with a list of personal information collected from children, and the opportunity to refuse further collection "from that child and to direct the operator to delete the child's personal information."	n/a	1798.99.31(a)(8). If the online service, product, or feature allows the child's parent, guardian, or any other consumer to monitor the child's online activity or track the child's location, provide an **obvious signal to the child** when the child is being monitored or tracked.	n/a	Sec. 4(b)(2). Covered platforms shall provide "readily-accessible and easy-to-use tools for parents", which shall include control of privacy and account settings (including limiting contacts with minor, preventing viewing of minor's persona data, and deleting the minor account), restricting purchases, tracking metrics, and addressing harms related to harms listed above.	Sec. 8. Manufacturers of connected devices directed to children or minors must provide a "dashboard" or label, either electronically or on the device's packaging w/r/t the collection, transmission, use, and security of the personal information of the child or minor.
Advertising [pp14-15]	16 C.F.R. § 312.2. Third party ad networks may not collect personal information (including persistent identifiers) from another online service when the ad network actually knows that the other service is directed at children. First-party services are also responsible for personal information collected from children on their behalf.	1798.140(ah). Consumers have the right to know or opt-out of "sharing," which is the disclosure of personal information "to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration."	1798.99.31(b)(2) A business shall not "[p]rofile a child by default" unless (A) "appropriate safeguards'' are in place, and (B) profiling is "necessary to provide the online service . . . with respect to the aspects of the online service, product, or feature with which the child is actively and knowingly engaged," or there is a "**compelling reason** that profiling is in the **best interests** of children."	Sec. 205(a). Targeted advertising is prohibited for an individual if the covered entity "has knowledge" that the individual is a covered minor; the level of knowledge varies for covered entities generally, large data holders, and high-impact social media companies. See *Covered Platforms and Entities* above.	Sec. 4(d). "A covered platform shall not facilitate the advertising of narcotic drugs . . . tobacco products, gambling, or alcohol to minors."	Sec. 6(a). **No targeted marketing to children or minors.** Operators of a service directed to children or minors may not engage in the "use, disclosure, or compiling of personal information [that] involves or is reasonably likely to involve collection of personal information" from a child or minor for "targeted marketing," except a minor may consent.

Additional topics covered in the primary chart include **Covered Data** [pp6-7], **Knowledge Standard with Respect to Conduct or Harm** [p8], **Impact Assessments** [pp16-17], **Consultation** [p18], and **Enforcement** [18].

Major U.S. Children's Online Safety Laws and Bills

	Children's Online Privacy Protection Act (15 U.S.C § 6501 et seq.)	California Privacy Rights Act (Cal. Civil Code § 1798.100 et seq.)	California Age-Appropriate Design Code Act (Cal. Civil Code § 1798.99.28 et seq.)	American Data Privacy and Protection Act (1117th, HR 8152)	Kids Online Safety Act (117th, S 3663)[1]	Children and Teens Online Privacy Protection Act (117th, S 1628)[2]
Overall Approach to Children's Privacy and Online Safety	Prohibits collecting personal information from children (under 13) without verifiable parental consent if directed to children or with actual knowledge	Prohibits sale or sharing of personal information with actual knowledge that the consumer is under 16 without consent by a parent (under 13) or the consumer (13 to 16)	Businesses providing online services likely to be accessed by children (under 18) must meet ten affirmative obligations centered on a Data Protection Impact Assessment and eight prohibitions	Prohibits targeted advertising to or the transfer of data of an individual with actual knowledge the individual is a covered minor (under 17); transfer may be done with parental or minor consent	Implements a duty of care for a covered platform to act in the best interests of minors (16 or under) if it is used or reasonably likely to be used by a minor, including "reasonable measures" to prevent specific harms	Extends COPPA to minors aged 13 to 17 and to services likely to be used by children or minors. Prohibits targeted marketing to children and minors. Allows minors to consent to collection of personal information and targeted advertising and requires a mechanism for users to erase public information posted by the user regarding a child.
Covered Users / Definition of "Child" or "Minor"	16 C.F.R. 312.2. A "child" is an individual **under the age of 13**.	1798.120(c). A consumer **under the age of 16**; consumers at least 13 and less than 16 may "affirmatively authorize" the sale or sharing, while parents may do so for consumers under 13. 1798.120(i). "Consumer" means a natural person who is a California resident.	1798.99.30(b)(1). "Child" is a consumer **under 18 years of age.**[3]	Sec. 2(11). A "covered minor" means an" individual under the age of 17."	Sec. 2(2) "Child" means an "individual who is age 12 or younger." (5) "Minor" means "an individual who is **age 16 or younger**." (**Minor** remains the catchall term for all users covered by the bill.)	Retains COPPA's definition of "child" (under 13). Sec. 3(a)(6). A "minor" is "an individual over the age of 12 and under the age of 17."[4]

[1] Notes here reflect the version of KOSA reported to the Senate on Dec. 15, 2022.
[2] Notes here reflect the version of COPPA 2.0 reported to the Senate on Dec. 15, 2022.
[3] The California Age Appropriate Design Code Act's legislative preamble states that businesses "should take into account" the news of the following age groups: 0 to 5, 6 to 9, 10 to 12, 13 to 15, and 16 to 17. However, "a preamble is not binding in the interpretation of the statute" and "may not overturn the statute's language," although it "can be illuminating if a statute is ambiguous." Yeager v. Blue Cross of Cal., 96 Cal. Rptr. 3d 723, 727 (2009).
[4] Highlighted text denotes substantive changes from COPPA.

Covered Platforms and Entities (including knowledge of child's age)	16 C.F.R. 312.3. An "operator of a Web site or online service **directed to children**, or any operator that has **actual knowledge** that it is collecting or maintaining personal information from a child" is prohibited from collecting personal information from a child without providing notice and receiving verifiable parental consent. 16 C.F.R. 312.2. Whether a website is "directed to children" depends on "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" as well as "**competent and reliable empirical evidence regarding audience composition**, and evidence regarding the intended audience." "Actual knowledge" w/r/t a child's age for first party services can be established: ● FAQ. E.g., "if you monitor user posts, if a responsible member of your organization sees the post, or if someone alerts you to the post" ● FTC v. Yelp. "accept[ing] registrations from users who input data of birth indicating they were under the age of 13." Does not include children's posts	1798.120(c). A business is prohibited from the sale or sharing of the personal information of a consumer under 16 if it has "**actual knowledge**" of the consumer's age without receiving consent 1798.120(c). **"Willful disregard"** of a child's age constitutes actual knowledge; Cal. AG declined to clarify that CCPA and COPPA provide the same standard, but stated that CCPA does "not require a business to investigate or inquire about age." FSOR, app'x A at 170, 269. 1798.140(d). A "business" is a for-profit legal entity that (1) "collects consumers' personal information, or on the benefit of which such information is collected," (2) "determines the purposes and means of the processing of consumers' personal information," (3) does business in California, and (4) meets one threshold for gross revenue ($25m), sale of personal information (100k consumers or households), or revenue from sale of personal information (50% or more).	1798.99.31(a). Applies to a "business" as defined in the CPRA, that "provides an online service, product, or feature **likely to be accessed by children**" No knowledge requirement w/r/t child's age. 1798.99.30(b)(4) **"Likely to be accessed by children"** means it is "reasonable to expect" that the service: (A) is "**directed to children** as defined by the Children's Online Privacy Protection Act (15 U.S.C. Sec. 6501 et seq.)" (B) is "routinely accessed by a **significant** number of children" based on "**competent and reliable evidence** regarding **audience composition**" (C) Feature "**advertisements marketed to children"** (D) "is substantially similar or the same as an online service, product, or feature subject to subparagraph (B)" (E) "has **design elements that are known to be of interest to children, including, but not limited to games, cartoons, music, and celebrities who appeal to children"** (F) has an audience, of which a "significant amount" **is "determined, based on internal company research, to be children"** (5) "Online service, produce, or	Sec. 205(a)-(b). A covered entity is subject to ADPPA's provisions regarding covered minors if it "**has knowledge**" that the individual is a covered minor. Sec. 2(20)(A). "Knowledge" varies depending on the entity: (i) for "high impact social media companies,"[5] it means "knew or should have known"; (ii) for large data holders, it means "knew or acted n willful disregard"[6] and, (iii) for all others, it means "actual knowledge" Sec. 2(9). A covered entity is "any entity or person, other than an individual acting in a non-commercial context" that (1) "determine the purposes and means of collection, processing, or transferring covered data," and (2) is subject to FTC jurisdiction, is a common carrier under the Communications Act, or is a non-profit. Excludes governmental entities, entities acting on their behalf (limited to that capacity), and any "congressionally designated nonprofit, national resources center, and clearinghouse . . . on missing and exploited children issues." Does not include service providers.	Sec. 2(3) ''Covered platform'' means a "social media service, social network, video game, messaging application, video streaming service, educational service, or an online platform that connects to the internet and that is used, or is **reasonably likely to be used, by a minor**." No knowledge requirement w/r/t child's age. Sec. 2(6) "Online platform" means "any public-facing website, online service, online application, or mobile application that primarily provides a community forum for user generated content, including sharing videos, images, games, audio files, or other content." Sec. 4(a)(2). Safeguards for Minors. "A covered platform shall provide that, in the case of a user that the platform **knows or reasonably believes** to be a **minor**, the default setting for any safeguard . . . shall be the option available on the platform that provides the most protective level of control that is offered by the platform over privacy and safety for that user." Sec. 4(b)(4) Parental tools "A covered platform shall provide that, in the case of a user that the platform **knows or reasonably believes** to be a **child**, the tools described in this subsection shall be enabled by default." See	Sec. An operator of an online service is prohibited from collecting personal information from a child or minor if the service is "directed to children or minors or is used or **reasonably likely to be used by children or minors**" prior to obtaining "verifiable consent" from the minor or the parent of a child. Sec. 3(d)(2). Now includes **common carriers** as defined by Communications Act of 1934. Sec. 3(a)(6). "Directed to children **or minors**" retains considerations identified in COPPA rules, but adds "**advertising content used on, or used to advertise" the service**." Sect. 3(a)(6). "Reasonably likely to be used" is defined by the FTC. **"Actual knowledge" has been removed.** Sec. 3(a)(1). An "operator" is any person (i) "who, for commercial purposes . . . operates or provides a website on the **internet, an online service, an online application, a mobile application, or a connected device**" and (ii) "collects or maintains, either directly or through a service provider, personal information from or about the users," permits others to do so, or **allows users to publicly disclose personal information**.

	Children's Online Privacy Protection Act (15 U.S.C § 6501 et seq.)	California Privacy Rights Act (Cal. Civil Code § 1798.100 et seq.)	California Age-Appropriate Design Code Act (Cal. Civil Code § 1798.99.28 et seq.)	American Data Privacy and Protection Act (1117th, HR 8152)	Kids Online Safety Act (117th, S 3663)[1]	Children and Teens Online Privacy Protection Act (117th, S 1628)[2]
	"if no one in your organization is aware of the post." 16 C.F.R. 312.2. An "operator" is "any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service" or on whose behalf personal information is **collected or maintained**. "[C]hild-directed sites or services whose primary target audience is children must continue to presume all users are children and to provide COPPA protections accordingly," unless it's a mixed audience site. Final rule amendments, 78 Fed. Reg. 3972, 3984 (Jan. 17, 2013). 16 C.F.R. 312.2. A third party service is **directed to children** if it has **actual knowledge** it is collecting personal information from another service directed to children.		feature" does not include: (A) broadband internet access service, as defined in Section 3100. (B) telecommunications service, as defined in Section 153 of Title 47 of the US Code (C) The delivery or use of a physical product.		*Parental Supervision Tools* for more on the safeguards.	Sec. 9. The operators of a service directed to children or minors "shall treat each user of that [service] as a child or minor, except as permitted by the Commission pursuant to a regulation promulgated under this Act, and except to the extent the website, online service, online application, mobile application, or connected device is deemed directed to mixed audiences." Reflects "presumption" reiterated by FTC in COPPA rulemaking, but not included in COPPA rule. Sec. 3(a)(6). A third party service is **directed to children** if the other service from which it collects personal information is (I) directed to children or minors or (II) used or reasonably likely to be used by minors. **Removes the actual knowledge requirement for third parties.**

[5] Under the ADPPA, a "covered high-impact social media company" is a covered entity that provides "any internet-accessible platform" that (1) generates $3 billion or more in annual revenue, (2) has 300 million or more monthly active users for "not fewer" than three of the preceding 12 months, and (3) is used primarily by users to access or shar user-generated content. Sec. 2(9)(B).

[6] Under the ADPPA, a "large data holder" is a covered entity that in the most recent calendar year, (1) had annual gross revenue of $250 million or more and (2) processed the covered data of more than 5 million people or devices **and** the sensitive data of 200,000 individuals or devices. Sec. 2(1)(A)

	Children's Online Privacy Protection Act (15 U.S.C § 6501 et seq.)	California Privacy Rights Act (Cal. Civil Code § 1798.100 et seq.)	California Age-Appropriate Design Code Act (Cal. Civil Code § 1798.99.28 et seq.)	American Data Privacy and Protection Act (1117th, HR 8152)	Kids Online Safety Act (117th, S 3663)[1]	Children and Teens Online Privacy Protection Act (117th, S 1628)[2]
Covered Data	"Personal information" is "individually identifiable information about an individual collected online," including name, physical address or street-level geolocation, online contact information, persistent identifiers, photographs or audio files, and parents' names. Personal information under COPPA must be "from" a child, but does not have to regard the child.	1798.120(c). Personal information is "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," including identifiers such a real name, IP address, email address, protected characteristics, biometric information, geolocation data, education information under FERPA, and certain sensitive personal information.	"Personal information" as defined by the CPRA.	Sec. 2(8). "Covered data" means information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual, and may include derived data and unique persistent identifiers." Excludes de-identified data and employee data.	Sec. 2(6). "Personal data" means information that identifies or is linked or reasonably linkable to an individual, household, or consumer device.	Same as under COPPA, but broadens **biometrics**, defined as "measurement or technological processing of an individual's biological, physical, or physiological characteristics."

	Children's Online Privacy Protection Act (15 U.S.C § 6501 et seq.)	California Privacy Rights Act (Cal. Civil Code § 1798.100 et seq.)	California Age-Appropriate Design Code Act (Cal. Civil Code § 1798.99.28 et seq.)	American Data Privacy and Protection Act (1117th, HR 8152)	Kids Online Safety Act (117th, S 3663)[1]	Children and Teens Online Privacy Protection Act (117th, S 1628)[2]
Age Verification or Estimation	Does not require investigation of ages. 1999 Statement of Basis and Purpose, 64 Fed. Reg. 59888, 59889 (Apr. 21, 2000). 16 C.F.R. 312.2 & FAQs. "Mixed audience" services, which are directed to children, but do not "target children as [their] primary audience" may implement an age gate to "collect[] age information" from users and "[p]revent[] the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13"	Cal. AG stated that CCPA does "not require a business to investigate or inquire about age." FSOR, app'x A at 170.	1798.99.31(a)(1)(5). Businesses must "[e]stimate the age of child users with a **reasonable level of certainty appropriate to the risks** that arise from the data management practices of the business or apply the privacy and data protections afforded to children to all consumers." 1798.99.31(b)(8). A business shall not "[u]se any personal information collected to estimate age or age range **for any other purpose** or retain that personal information longer than necessary to estimate age. **Age assurance shall be proportionate to the risks and data practice of an online service, product, or feature**." 1798.99.32(d)(3). The working group shall ensure "that age assurance methods . . . **are proportionate to the risks** that arise from the data management practices of the business, privacy protective, and minimally invasive."	Unclear. Although the "actual knowledge" standard applied by the ADPPA to covered entities generally likely does not require age verification, it is not clear how the "willful disregard" and "knew or should have known" standards for large data holders and high-impact social media companies would be interpreted.	Sec. 6(c)(1)(C). Annual report must account for the number of individuals using the covered platform reasonably believed to be minors in the US, disaggregated by the age ranges of 0-5, 6-9, 10-12, 13-16. Sec. 9. NIST, with FCC, FTC, and Commerce to conduct a study evaluating the most technologically feasible options for developing systems to verify age at the device or operating system level.	Retains provisions in COPPA rule for mixed audience services.

	Children's Online Privacy Protection Act (15 U.S.C § 6501 et seq.)	California Privacy Rights Act (Cal. Civil Code § 1798.100 et seq.)	California Age-Appropriate Design Code Act (Cal. Civil Code § 1798.99.28 et seq.)	American Data Privacy and Protection Act (1117th, HR 8152)	Kids Online Safety Act (117th, S 3663)[1]	Children and Teens Online Privacy Protection Act (117th, S 1628)[2]
Knowledge Standard with Respect to Conduct or Harms	Same as knowledge with respect to age. May not knowingly collect or maintain personal information from a child.	Same as knowledge with respect to age. May not knowingly sell or share personal information from a consumer under 16. 1798.135(c)(5). Must wait 12 months before again requesting a consumer under 16 to consent to sale or sharing of personal information. 1798.155(a). Enhanced penalties in administrative enforcement for **intentional** violations or violations involving the personal information of consumers for whom the business "has **actual knowledge** are under 16 years of age."	1798.99.31(b) A business shall not: (1) "Use the personal information of any child in a way that the business **knows, or has reason to know,** is materially detrimental to the physical health, mental health, or well-being of a child." (7) "Use dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected . . . 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." 1798.99.35(a). Penalties for **negligent** violations; enhanced penalties for **intentional** violations.	Same as knowledge with respect to age.	Sec. 3(a). Covered platforms "shall take **reasonable measures** in its operation of products and service" to mitigate listed harms. See *Duty of Care*.	Same as knowledge with respect to age.

Privacy and Security Obligations Including Notice	16 C.F.R. 312.3. Operators of a service directed at children or with actual knowledge it is collecting or maintaining personal information from a child may not collect or maintain personal information from a child. 16 C.F.R. 312.4(a)-(c). Must provide **direct notice** to a parent prior to collecting or maintaining personal information from a child. 16 C.F.R. 312.4(d). Must provide public notice of "its information practices with regard to children" prior to collecting or maintaining personal information from a child. 16 C.F.R. 312.6(a). Must provide parents with a **list of personal information collected** from children, and the opportunity to **refuse further collection** "from that child and to direct the operator to **delete** the child's personal information." 16 C.F.R. 312.7. Operators **may not condition** "a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary." 16 C.F.R. 312.8. Operators must "establish and maintain reasonable procedures to protect the **confidentiality, security, and integrity** of personal information collected from children."	**Child-specific:** 1798.120(c). Consumers under the age of 16 have the right to opt-in to the sale or sharing of their personal information. 1798.100(a). A business must provide notice of the categories of personal information to be collected and the purposes of its use (not limited to children). 1798.100(c). Use, retention, and sharing must be reasonably proportionate to the intended purpose (not limited to children). 1798.105. Consumers have the **right to delete** personal information (not limited to children). 1798.106. Consumers have the right to request the **correction** of inaccurate personal information (not limited to children). 1798.110. Consumers have the right to request that a business **disclose the categories of personal information collected**, its sources, its purpose, its recipients, and specific personal information about the requesting consumer (not limited to children). 1798.115(a), (c) Must **disclose sale or sharing of personal information** to third parties, service providers, or contractors (not limited to children).	1798.99.31(a). Businesses must: (6) "Configure all default privacy settings provided to children . . . to settings that offer a **high level of privacy**, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children." (7) "Provide any **privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age** of children likely to access that online service, product, or feature." (9) "**Enforce published terms, policies, and community standards** established by the business, including, but not limited to, privacy policies and those concerning children." (10) "**Provide prominent, accessible, and responsive tools** to help children, or if applicable their parents or guardians, exercise their privacy rights and report concerns."	**Child-specific:** Sec. 205(a). Covered entities may not engage in targeted advertising to any individual with respect to whom the entity "has knowledge" is a "covered minor." **Child-specific:** Sec. 205(b). "A covered entity may not transfer or direct the transfer" of a covered minor's covered data if the covered entity has knowledge the individual is a covered minor and has not obtained "affirmative express consent" from the covered minor or their parent. Exceptions for transfer of information relating to child victimization to law enforcement or a congressionally designated nonprofit, national resource center and clearinghouse on missing and exploited children. **Child-specific:** Sec. 406(b). FTC must update COPPA rule within 180 days. Sec. 101(a). Data collected, processed, or transferred is limited to what is "reasonably necessary and proportionate" to "provide or maintain the specific product or service requested by the individual" or for specific permitted purposes. Sec. 102. Limits on collection and transfer of specific information, including sensitive covered data. Sec. 103. Establishment of policies and procedures to mitigate	Sec. 5(a)(1). Covered platforms must provide notice, prior to "registration, use, or purchase" by a minor," of: (A) the platform's "policies and practices" w/r/t "personal data and safeguards for minors"; (B) accessing the safeguards and parental tools in section 4; and, (C) whether the platform and "any algorithmic recommendation system" pose "any heightened risks of harms to minors." Sec. 5(a)(2)-(3). "For a minor, or an individual that a covered platform reasonably believes is a minor," must provide notice to a parent and "take reasonable steps to obtain express affirmative acknowledgement" of receipt of notice. Sec. 5(b). Cover platform that operates "algorithmic recommendation systems that use minors' personal data" shall provide notice with overview of systems and "options for minors or their parents to control" the systems.	Sec. 3(b)(3)(A). Retains and slightly expands COPPA provisions regarding notice and verifiable consent; must provide minors and parents of children: (I) "description of the specific types of personal information collected" from the minor or child; (II) opportunity to "delete personal information collected" from the minor or child and "refuse further use or collection"; (III) "reasonable" means to "obtain any personal information collected from" the minor or child. Must now "prevent the collection" of more personal information from a minor or child than "is reasonably required" to use the online service. Does not address COPPA rule's prohibition on unnecessary retention. Retains provisions regarding "confidentiality, security, and integrity of personal information." Sec. 4. Incorporates Fair Information Practice Principles of (1) collection limitation, (2) data quality, (3) purpose specification, (4) retention limitation, (5) security and safeguards, (6) transparency, (7) individual participation and consent, and (8) prohibiting racial and socioeconomic profiling. Sec. 7(b). Operators must provide

	Children's Online Privacy Protection Act (15 U.S.C § 6501 et seq.)	California Privacy Rights Act (Cal. Civil Code § 1798.100 et seq.)	California Age-Appropriate Design Code Act (Cal. Civil Code § 1798.99.28 et seq.)	American Data Privacy and Protection Act (1117th, HR 8152)	Kids Online Safety Act (117th, S 3663)[1]	Children and Teens Online Privacy Protection Act (117th, S 1628)[2]
	16 C.F.R. 312.10. Operators "shall **retain** personal information collected online from a child for **only as long as is reasonably necessary** to fulfill the purpose for which the information was collected. The operator must delete such information using reasonable measures . . . ."	1798.120. Consumers have the right to opt-out of the sale or sharing of their personal information; **right for consumers under 16 to opt-in**. 1798.121. Right to **limit uses of "sensitive personal information"** to that "which is necessary to perform the services or provide the goods reasonably expected by an average consumer" (not limited to children) 1798.125. Businesses **may not discriminate** against a user exercising these rights, but may charge different prices if "reasonably related to the value" of the consumer's data (not limited to children). 1798.135(b). Businesses may utilize a global opt-out signal.		privacy risks in "design, development, and implementation of such products and services." Sec. 104. Prohibits retaliation for exercising ADPPA rights, including charging different prices or rate, except for "bona fide loyalty programs" and for offering differing pricing or functions w/r/t an individual exercising their right to delete. Sec. 202. Requires privacy policies, including short form notice by large data holders. Sec. 203. Rights of access, correction, deletion, and portability. Sec. 204. Rights to consent and opt out of data transfers and targeted advertising. Sec. 206. Notices by third-party collecting entities. Sec. 207(a). Prohibits collecting, processing, or transferring covered data in a manner that "discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability."		a mechanism that allows users to (1)(A) "erase or otherwise eliminate content or information" that is (i) submitted by that user, (ii) publicly available through that website, and (iii) contains or displays personal information of children or minors, unless (2) maintenance of the information is required by state or federal law or was submitted by another person other than the user requesting the information's erasure.

	Children's Online Privacy Protection Act (15 U.S.C § 6501 et seq.)	California Privacy Rights Act (Cal. Civil Code § 1798.100 et seq.)	California Age-Appropriate Design Code Act (Cal. Civil Code § 1798.99.28 et seq.)	American Data Privacy and Protection Act (1117th, HR 8152)	Kids Online Safety Act (117th, S 3663)[1]	Children and Teens Online Privacy Protection Act (117th, S 1628)[2]
				Sec. 208(a). Must establish "reasonable administrative, technical, and physical data security practices." Sec. 210. Global opt-out mechanisms for exercising rights to opt out of transfers of covered data and targeted advertising and to register for the "Do Not Collect" registry.		

	Children's Online Privacy Protection Act (15 U.S.C § 6501 et seq.)	California Privacy Rights Act (Cal. Civil Code § 1798.100 et seq.)	California Age-Appropriate Design Code Act (Cal. Civil Code § 1798.99.28 et seq.)	American Data Privacy and Protection Act (1117th, HR 8152)	Kids Online Safety Act (117th, S 3663)[1]	Children and Teens Online Privacy Protection Act (117th, S 1628)[2]
Duty of Care Obligations (e.g., a free standing design duty)	n/a	1798.185(a)(15). Businesses must file a risk assessment with the California Privacy Protection Agency. See *Impact Assessments, Reporting, and Transparency Obligations* below.	Cal. AADC Act omits the UK version's obligation to act in the "best interests of the child." However, the codified statutory declaration states that businesses "should consider the best interests of children," 1798.99.29(a); the legislative findings also state that California businesses may look to guidance provided by the United Kingdom's Information Commissioner's Office.[7] 1798.99.30(b)(2). In addition, businesses are required to conduct a "Data Protection Impact Assessment" to "assess and mitigate risks that arise from the data management practices of the business," including exposure to "harmful" content, contacts, and conduct. See *Impact Assessments, Reporting, and Transparency Obligations* below.	**Child-specific:** Sec. 103(a)(b). Covered entities must establish "reasonable policies, practices, and procedures" to "identify, assess, and mitigate privacy risks related to covered minors . . . to result in reasonably necessary and proportionate residual risk to covered minors" in "a manner that considers the developmental needs of different age ranges of covered minors."	Sec. 3(a). "A covered platform shall act in the best interests of a minor that uses the platform's products or services, as described in subsection (b)." (b) Prevention of Harms to Minors. "In acting in the best interests of a minor, a covered platform has a duty to take reasonable measures in its design and operation of products and services to prevent and mitigate physical, mental, financial, developmental or other material harms to minors," including (1) "mental health disorders . . . including self-harm, suicide, eating disorders, and substance use disorders"; (2) "patterns of use that indicate or encourage addiction-like behaviors"; (3) "physical harm, online bullying, harassment"; (4) "sexual exploitation, including enticement, grooming, sex trafficking, sexual abuse of minors and trafficking of online child sexual abuse material"; (5) "promotion and marketing of narcotic drugs . . . tobacco products, gambling, or alcohol"; and (6) "predatory, unfair, or deceptive marketing practices."	n/a

[7] Legislative declarations and preambles are not legally binding but may "illuminat[e]" ambiguous statutes. *Yeager*, 96 Cal. Rptr. 3d at 727.

	Children's Online Privacy Protection Act (15 U.S.C § 6501 et seq.)	California Privacy Rights Act (Cal. Civil Code § 1798.100 et seq.)	California Age-Appropriate Design Code Act (Cal. Civil Code § 1798.99.28 et seq.)	American Data Privacy and Protection Act (1117th, HR 8152)	Kids Online Safety Act (117th, S 3663)[1]	Children and Teens Online Privacy Protection Act (117th, S 1628)[2]
Role of Consent	16 C.F.R. 312.5(b). "Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent." 16 C.F.R. 312.5(a), (c) and FAQs. "Verifiable parental consent" must be obtained prior to collecting or maintaining personal information from a child, utilizing one of eight approved methods, including use of a credit card, video conferencing, checking a government-issued ID against a database, knowledge based challenge questions, and using facial recognition technology to compare a photo and government ID.	1798.120(d). A minor at least 13 and under 16 may consent to sale or sharing of their personal information; parents may consent for a consumer less than 13. Cal. Code Regs., tit. 11, § 7070. Parental consent must be obtained through a method that is "reasonably calculated to ensure that the person providing consent is the child's parent or guardian," including use of a credit card, video conferencing, in person communication, and checking a government ID against a database.	No consent provisions.	**Child-specific:** Sec. 205(b). Consent must be provided to transfer a covered minor's covered data. Sec. 101(a). Data collection, processing, and transferring limited to providing or maintaining a product or service "requested by the individual" (or other listed permissible purposes). Sec. 102(3). Consent is required to transfer sensitive covered data.	Limited consent provisions: Sec. 8. FTC to develop a standard consent form for market- and product-focused research on minors.	Sec. 3(a)(4). Retains COPPA's statutory definition of verifiable consent: Minor and parents of children may provide "verifiable consent," defined as "any reasonable effort (taking into consideration available technology)" that ensure that (A) the minor or parent receives "specific notice" of the operator's collection, use, and disclosure of personal information, and (B) is obtained before the collection of personal information from a minor or child. Sec. 3(a)(3)(A). FTC to promulgate regulations.

Parental Supervision Tools	16 C.F.R. 312.4(a)-(c). Must provide direct notice to a parent prior to collecting or maintaining personal information from a child. 16 C.F.R. 312.6(a). Must provide parents with a list of personal information collected from children, and the opportunity to refuse further collection "from that child and to direct the operator to delete the child's personal information."	n/a	1798.99.31(a)(8). If the online service, product, or feature allows the child's parent, guardian, or any other consumer to monitor the child's online activity or track the child's location, provide an **obvious signal to the child** when the child is being monitored or tracked.	n/a	Sec. 4(a)(1). A covered platform "shall provide a minor with readily accessible and easy-to-use safeguards" to: (A) limit the ability of other to "contact or find the minor, in particular individuals aged 17 or over with no relationship to the minor"; (B) "prevent other users . . . from viewing the minor's personal data collected by or shared on the covered platform, in particular restricting public access to personal data"; (C) "limit features that increase, sustain, or extend use of the covered platform by a minor"; (D) "control algorithmic recommendation systems that use a minor's personal data," including opting out; (E) delete the minor's account and personal data; (F) "restrict the sharing of the geolocation of a minor and provide notice regarding the tracking of a minor's geolocation"; and (G) "limit the amount of time spent by a minor on the covered platform." (2) Safeguards must default to the highest setting for individuals the platform "knows or reasonably believes to be a minor." Sec. 4(b)(2). Covered platforms shall provide "readily-accessible and easy-to-use tools for parents", which shall include: (A) " ability to control privacy	See notice and access rights for children in *Privacy and Security Obligations*. Sec. 8. Manufacturers of connected devices directed to children or minors must provide a "dashboard" either electronically or on the device's packaging of the collection, transmission, use, and security of the personal information of the child or minor.

	Children's Online Privacy Protection Act (15 U.S.C § 6501 et seq.)	California Privacy Rights Act (Cal. Civil Code § 1798.100 et seq.)	California Age-Appropriate Design Code Act (Cal. Civil Code § 1798.99.28 et seq.)	American Data Privacy and Protection Act (1117th, HR 8152)	Kids Online Safety Act (117th, S 3663)[1]	Children and Teens Online Privacy Protection Act (117th, S 1628)[2]
					and account settings, including safeguards established under (a)(1)"; (B) "ability to restrict purchases and financial transactions by a minor"; (C) "ability to track metrics of total time spent on the platform"; (D) "control options that allow parents to address the harms described in section 3(b)." (3) Notice to minors – "A covered platform shall provide clear and conspicuous notice to a minor when tools described in this subsection are in effect." (4) Default tools – "A covered platform shall provide that, in the case of a user that the platform knows or reasonably believes to be a **child**, the tools described in this subsection shall be enabled by default." Sec. 4(e). Must provide "information and control options in a clear and conspicuous manner that takes into consideration the differing ages, capacities, and developmental needs of the minors most likely to access the covered platform and does not encourage minors or parents to weaken or disable safeguards or parental controls." Dark patterns prohibited.	

	Children's Online Privacy Protection Act (15 U.S.C § 6501 et seq.)	California Privacy Rights Act (Cal. Civil Code § 1798.100 et seq.)	California Age-Appropriate Design Code Act (Cal. Civil Code § 1798.99.28 et seq.)	American Data Privacy and Protection Act (1117th, HR 8152)	Kids Online Safety Act (117th, S 3663)[1]	Children and Teens Online Privacy Protection Act (117th, S 1628)[2]
					Sec. 4(e)(3). Parental tools do not "require the disclosure of a minor's browsing behavior, search history, messages, or other content of their communications."	

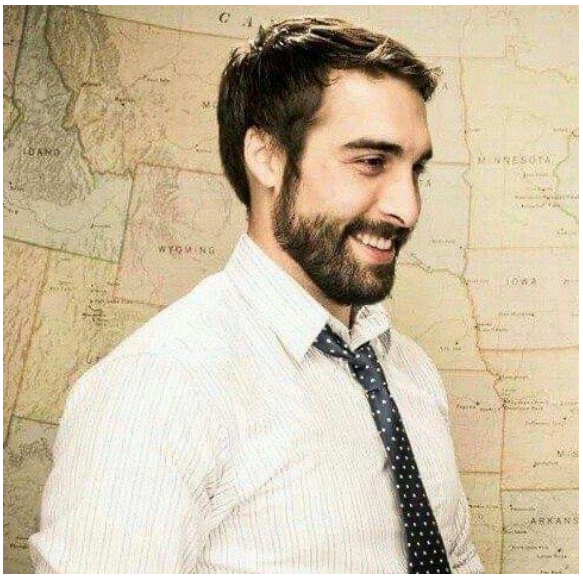
Advertising	16 C.F.R. § 312.2. Third party ad networks may not collect personal information (including persistent identifiers) from another online service when the ad network actually knows that the other service is directed at children. First-party services are also responsible for personal information collected from children on their behalf.	1798.140(ah). Several provisions allow consumers the right to know or opt-out of "sharing," which is the disclosure of personal information "to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration."	Sec. 1798.99.30(b)(6) "Profiling" means "any form of automated processing of personal information . . . to evaluate certain aspects relating to a natural person, including analyzing or predicting aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements." 1798.99.31(b) A business shall not: (2) "Profile a child by default" unless (A) "appropriate safeguards" are in place, and (B) profiling is "necessary to provide the online service . . . with respect to the aspects of the online service, product, or feature with which the child is actively and knowingly engaged," or there is a "**compelling reason** that profiling is in the **best interests** of children." (3) "Collect, sell, share, or retain any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged . . . unless the business can demonstrate a compelling reason that the collecting, selling, sharing, or retaining of the personal information is in the **best interests** of children . . . ."	Sec. 205(a). Targeted advertising is prohibited for an individual if the covered entity "has knowledge" that the individual is a covered minor; the level of knowledge varies for covered entities generally, large data holders, and high-impact social media companies. See *Covered Platforms and Entities* above.	Sec. 3(b)(5)-(6). Covered platforms must act in the best interest of a minor and "prevent and mitigate" harms associated with promotion and marketing of "narcotic, drugs . . . tobacco products, gambling, or alcohol" and "predatory, unfair, or deceptive marketing practices." Sec. 4(d). "A covered platform shall not facilitate the advertising of narcotic drugs . . . tobacco products, gambling, or alcohol to minors." Sec. 5(c). Covered platform "that facilitates advertising aimed at minors shall provide clear, conspicuous, and easy-to-understand information and labels on advertisements and marketing material" regarding: (1) "the name of the product, service, or brand and the subject matter of an advertisement or marketing material"; (2) "why the minor is being targeted for a particular advertisement or marketing material if the covered platform engages in targeted advertising, including material information about how the minor's personal data was used to target the advertisement or marketing material"; and (3) whether particular media is an advertisement or marketing material.	Sec. 6(a)(1). **No targeted advertising to children.** Operators of a service directed to children may not engage in the "use, disclosure, or compiling of personal information [that] involves or is reasonably likely to involve collection of personal information from a child" for "targeted marketing." Sec. 6(a)(2). **No targeted advertising to minors without verifiable consent**. Operators of a service director to minors may not "collect, use, disclose to third parties, or compile personal information" of a user who "is or is reasonably likely to be a minor" for "targeted marketing" prior to obtaining verifiable consent of the minor.

Impact Assessments and Reporting	n/a	1798.185(a)(15). Businesses must file a risk assessment with the California Privacy Protection Agency, "including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing." Cal. Code Regs., tit. 11, § 7101. Businesses must maintain records on consumer requests and their responses for 24 months, which may be used only for record-keeping purposes.	1798.99.30(b)(2) "Data Protection Impact Assessment" means a "systematic survey to assess and mitigate risks that arise from the data management practices of the business . . . ." 1798.99.31(a)(1) The business must: (A) Complete a DPIA before offering any online service likely to be accessed by children to the public and maintain documentation of this assessment as long as the service is likely to be accessed by children. Biennially review all DPIAs. (B) DPIA shall identify purpose of service, how it uses children's personal information, and the risks of "material detriment to children that arise from the data management practices of the business"; must also address whether the design of the service could: (i) harm children, including by exposing children to **"harmful, or potentially harmful, content** on the online product, service, or feature; (ii) "lead to children experiencing or being targeted by harmful, or potentially harmful, **contacts**"; (iii) "**permit children to witness, participate in, or be subject to harmful, or**	**Child-specific:** Sec. 207(c). Requires algorithmic impact assessments by large data holders, including mitigation of harms to covered minors. Sec. 208(b). Security assessments and preventative actions. Sec. 301(d)-(e). Requires privacy impact assessments, including the nature and risks posed by covered data collected, processed and transferred.	Sec. 4(c). Covered platforms shall provide a "readily-accessible and easy-to-use means to submit reports" of "harms to minors." Must respond within 14 days. Sec. 6(a). "[N]ot less frequently than once a year, a covered platform shall issue a public report identifying the foreseeable risks of harm to minors and describing the prevention and mitigation measures taken to address such risks based on an independent, third party audit conducted through reasonable inspection of the covered platform." (c)Content: (1) Transparency regarding (A) extent to which the platform is likely to be accessed by minors; (B) platform's commercial interests; (C) number of individuals using the covered platform reasonably believed to be minors in the US disaggregated by the age ranges of 0-5, 6-9, 10-12, 13-16; (D) median and mean amounts of time spent on the platform by minors in the US by above age ranges; (E) accounting, disaggregated by category of harms described in Sec. 3(b) of (i) total number of reports of the dissemination of illegal or harmful content involving minors, and **(ii) prevalence of content that is illegal or**	n/a

			potentially harmful, conduct"; (iv) "allow children to be party to or exploited by a harmful, or potentially harmful, contact"; (v) allows "algorithms used by the online product . . . [to] harm children"; (vi) allows "targeted advertising systems used by the online product . . . [to] harm children"; (vii) allows "system design features to increase, sustain, or extend use of the online product . . . including the automatic playing of media, rewards for time spent, and notifications"; (viii) "collect[] or process[] sensitive personal information of children." (2) Create a "timed plan" to "mitigate" risks documented in DPIA (3) Provide a list of all DPIAs to AG within three days upon request (4) Provide a specific DPIA to AG within five days upon request.[8] (7) "Provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service, product, or feature."		**harmful to minors;** (F) description of any material breaches of parental tools; (2) Systemic risks assessment regarding (A) audit for reasonably foreseeable risks to minors; (B) how algorithmic recommendation systems and targeted advertising can harm minors; (C) how design feature "increase, sustain, or extend use of a product or service by a minor"; (D) how and for what purpose platform processes personal data that may harm minors; (E) evaluation of safeguards and parental tools under section 4; (5) other matters of public concern; (3) Mitigation, including descriptions of (A) safeguards and parental tools; (B) interventions by covered platform; (C) prevention and mitigation measure in response to "known and emerging risks"; (D) process for handling reports of harms to minors; (E) implementation of prevention and mitigation measures; and (F) "additional measures to be taken by the covered platform to address the circumvention of safeguards for minors and parental tools"	

	Children's Online Privacy Protection Act (15 U.S.C § 6501 et seq.)	California Privacy Rights Act (Cal. Civil Code § 1798.100 et seq.)	California Age-Appropriate Design Code Act (Cal. Civil Code § 1798.99.28 et seq.)	American Data Privacy and Protection Act (1117th, HR 8152)	Kids Online Safety Act (117th, S 3663)[1]	Children and Teens Online Privacy Protection Act (117th, S 1628)[2]
Consultation	n/a	n/a	1798.99.32(b) Working Group members shall consist of Californians with expertise in at least two of the following areas: (1) Children's data privacy; (2) physical health; (3) mental health and well-being; (4) computer science; (5) children's rights.	FTC required to consult with NIST in promulgating rules for rights to access, correct, delete, and port covered data, with the Secretary of Commerce for guidance and rules regarding ADPPA's civil rights rules, and with civil rights agencies for civil rights enforcement.	Sec. 12(b). The Kids Online Safety Council shall include diverse participation from: (1) academic experts, health professionals, members of civil society with expertise in mental health and the prevention of harms to minors; (2) academia and civil society with specific expertise in privacy and civil liberties; (3) parents and youth; (4) covered platforms; (5) NTIA, NIST, FTC, DOJ, HHS; (6) state AGs or designees	n/a

	Children's Online Privacy Protection Act (15 U.S.C § 6501 et seq.)	California Privacy Rights Act (Cal. Civil Code § 1798.100 et seq.)	California Age-Appropriate Design Code Act (Cal. Civil Code § 1798.99.28 et seq.)	American Data Privacy and Protection Act (1117th, HR 8152)	Kids Online Safety Act (117th, S 3663)[1]	Children and Teens Online Privacy Protection Act (117th, S 1628)[2]
Enforcement	15 U.S.C. 6504-05. FTC and State AGs. § 312.9 A violation of the COPPA rule "shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act."	1798.155. California Privacy Protection Agency, with enhanced penalties for selling or sharing the personal information of a consumer under 16.	California Attorney General. 1798.99.35(a). Any business found to violate the CA AADC will be subject to an injunction and "liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) per affected child for each **negligent** violation or not more than seven thousand five hundred dollars ($7,500) per affected child for each **intentional** violation". 1798.99.35 (c) (1) If a business is in substantial compliance with the requirements of paragraphs (1) through (4), inclusive, of subdivision (a) of Section 1798.99.31, the Attorney General shall provide written notice to the business, before initiating an action under this title, identifying the specific provisions of this title that the Attorney General alleges have been or are being violated.	Secs. 401-03. Enforcement by FTC, State AGs, and individuals. Sec. 401(c). "A violation of this Act or a regulation promulgated under this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the13 Federal Trade Commission Act."	Sec. 11(a). FTC as a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act. (b) State Attorneys General in civil action if "the attorney general of a State has **reason to believe that an interest of the residents of that State has been or is threatened or adversely affected** by the engagement of any person in a practice that violates this Act or a regulation."	Sec. 12(a). FTC as a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act



Cody Venzke

Senior Counsel, Equity in Civic Technology

Cody Venzke is a Senior Counsel for CDT's Equity in Civic Technology Project, where he works to ensure that education agencies and other civic institutions use technology responsibly and equitably while protecting the privacy and civil rights of individuals. He is a contributor to the California Lawyers Association's treatise on the California Consumer Privacy Act, including on the right to opt out and compliance with recordkeeping and training requirements.

Prior to joining CDT, Cody served as an Attorney Advisor at the Federal Communications Commission and clerked for the Honorable Julio M. Fuentes on the Third Circuit and the Honorable Jan E. DuBois in the Eastern District of Pennsylvania. Cody also worked on the litigation team of an international law firm, where he served clients in emerging technologies such as clean energy, medicine, and media. In his pro bono work, Cody has represented tenants in eviction actions, assisted applicants under the U visa program, and supported litigation to ensure criminal defendants receive adequate representation under the Fifth Amendment. Prior to starting his law career, Cody taught math at a large public high school in Houston, Texas through Teach For America.

Cody graduated from St. Olaf College and Stanford Law School, and grew up in rural Iowa.

Tyler G. Newby

415-875-2495
tnewby@fenwick.com

Partner
Litigation

Office
San Francisco

Tyler focuses his practice on privacy and data security litigation, counseling and investigations, as well as intellectual property and commercial disputes affecting high technology and consumer-facing companies. Tyler has an active practice in defending companies in consumer class actions, state attorney general investigations and federal regulatory agency investigations arising out of privacy and data security incidents. In addition to his litigation practice, Tyler regularly advises companies large and small on reducing their litigation risk on privacy, data security and secondary liability issues. Tyler frequently counsels companies on compliance issues relating to key federal regulations such as the Children's Online Privacy Protection Act (COPPA), the Fair Credit Reporting Act (FCRA), the Computer Fraud and Abuse Act (CFAA), the Gramm Leach Bliley Act (GLBA), Electronic Communications Privacy Act (ECPA), the General Data Protection Regulation (GDPR), the Telephone Consumer Protection Act (TCPA), and state privacy laws, including the California Consumer Privacy Act (CCPA).

In 2014, Tyler was named among the top privacy attorneys in the United States under the age of 40 by *Law360*. Tyler is a member of the International Association of Privacy Professionals, and has received the CIPP/US certification. He previously served as a Chair of the American Bar Association Litigation Section's Privacy & Data Security Committee, and as a member of the ABA's Cybersecurity Legal Task Force.

"There are increasingly complex state laws and foreign statutes, and even small startups have global footprints now. We're trying to anticipate what our clients' needs will be in the coming years."

Tyler Newby
Daily Journal, "Top Cyber Lawyers 2019"

Practices

- Litigation
- Privacy & Cybersecurity
- Public Companies
- Securities Enforcement
- White Collar & Regulatory Defense
- Commercial Litigation
- Consumer Class Actions & Mass Arbitration

Industries

- Healthtech
- Games
- Autonomous Transportation & Robotics

Education & Admissions

- J.D., Stanford Law School
  Member, Notes Editor and Associate Editor, *Stanford Law Review*
- A.B., *summa cum laude*, History
  Dartmouth College
  Phi Beta Kappa
- Admitted to practice in California
- Admitted to practice before all federal district courts in California, the U.S. Courts of Appeals for the Federal Circuit and the U.S. Supreme Court

Representative Experience

Privacy, Data Security and E-Commerce Litigation

- Represent cloud computing services company in multi-district consumer class action arising out of data breach of customer's account.
- Advise and represent consumer internet companies in state and federal wiretapping individual and consumer class actions.
- Won dismissal of COPPA enforcement action brought by New Mexico Attorney General on behalf of two advertising technology companies.
- Represented advertising technology company and obtained favorable resolution of privacy class action brought on behalf of children players of popular mobile app game.
- Obtained dismissal of putative class action alleging false advertising claims associated with Intuit's TurboTax free filing option for tax preparation services. The Ninth Circuit reversed the district court's decision, noting TurboTax's terms of service were clearly visible when users signed in on its website, and that the terms included a clause requiring disputes to be resolved through arbitration. The panel instructed the district court to compel arbitration,

rejecting its alternative rationale that the users could bring a class action under a provision in the agreement that allows a court to award certain forms of equitable relief.

- Obtained dismissal of putative class action brought against internet security software developer alleging the software had been compromised from a prior cyberattack.
- Obtained dismissal of privacy class action against popular mobile radio streaming application.
- Representation of mobile application developers in putative consumer class action privacy and unfair competition cases.
- Obtained dismissal of putative class action alleging violations of California's Karnette Rental-Purchase Act and Unfair Competition Law Act brought against Resident Home, a company that owns and operates several direct-to-consumer brands in the home furnishings space, including Nectar and DreamCloud. The plaintiffs' petition for appeal was denied by the First District Court of Appeal.
- Obtained dismissal of consumer class action claim brought against business alleging violation of California's anti-spam law.
- Obtained dismissal at the pleading stage of putative class action brought against mobile application developer alleging violation of the Telephone Consumer Protection Act.

Privacy and E-Commerce Regulatory

- Representation of companies in investigations of network security breaches and advise companies on development and implementation of privacy and security programs.
- Negotiated resolution of COPPA enforcement action brought by New Jersey against social networking app developer.
- Represented major mobile advertising network in FTC investigation and enforcement action concerning inferring location data from Wi-Fi access points and compliance with COPPA.
- Advise numerous consumer-facing internet companies on development of law enforcement compliance programs and in responding to law enforcement and regulatory agency requests for consumer data.

- Representation of mobile device application developers in California Attorney General, U.S. DOJ and FTC privacy investigations.

Intellectual Property Litigation

- Representation of major B2B internet company in direct and secondary liability trademark infringement litigation.
- Representation of major video game publisher in copyright and computer fraud litigation concerning theft and distribution of pre-release version of game.
- Representation of computer device and component manufacturer in trademark infringement litigation over use of its house brand.
- Representation of mobile game publisher in trade secret litigation over hiring of software engineers.

Securities Regulatory and White Collar

- Representation of Fortune 100 company in internal investigation and related SEC and DOJ investigations into allegations of bribery and kick-back allegations.
- Representation of former public company officer in SEC Sarbanes-Oxley investigation and criminal prosecution.
- Internal investigation on behalf of audit committee into allegations of accounting and procurement improprieties.
- Representation of individuals in DOJ and SEC fraud and insider trading investigations and litigation.

Recognition

Recognition

Chambers AND PARTNERS

Chambers USA

2022

Privacy & Data Security - Nationwide.

The LEGAL 500

The Legal 500

2018 - 2022

Media, Technology and Telecoms: Cyber Law (including data privacy and data protection).

Daily Journal

The Daily Journal
2019

Named among 2019 Top Cybersecurity Lawyers in California.

Best Lawyers

U.S. News - Best Lawyers
2019-2021

Criminal Defense: White-Collar.