FUTURE OF PRIVACY FORUM

POLICY BRIEF:

Comparing the UK and California Age-Appropriate Design Codes

DECEMBER 2022

AUTHORED BY

Chloe Altieri
Policy Counsel

Bailey Sanchez
Policy Counsel

Christina Michelakaki
Policy Intern

Peyton Thomas
Policy Intern

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

EXECUTIVE SUMMARY

This policy brief provides a comparative analysis of the United Kingdom's Age Appropriate Design Code (UK AADC) and the California Age-Appropriate Design Code Act (California AADC). FPF published a policy brief with a summary and analysis of the California AADC, which is a first-of-its-kind privacy by design law in the United States that will become enforceable on July 1, 2024.

The California AADC was modeled after the UK AADC and key elements of the law were drawn from the text of the UK version. The UK AADC includes 15 standards for the safeguarding of children's privacy and exists under the framework of the UK's General Data Protection Regulation (GDPR). A key distinction between California AADC and UK AADC is the difference in their underlying regulatory frameworks. The UK AADC is a statutory code of practice under the UK GDPR, while the California AADC is a law that will be independently enforced. The California AADC is a novel approach to children's privacy in the US, and as businesses await further information from the California legislature, it may be useful to understand the points of comparison and divergences from the UK AADC.

This policy brief compares and analyzes the 15 standards of the UK AADC alongside the California AADC. Some key observations:

- **Guidance and tools for compliance:** In many instances, the California AADC leaves terms undefined or lacks further guidance on compliance. The UK AADC provides more explanation accompanying each standard.
- **"Best interests of the child":** The "best interests of the child" standard is a key piece of the UK AADC derived from the UN Convention on the Rights of the Child. The California AADC instead makes reference to "best interest of children" in the legislative findings and within exemptions to requirements rather than as an independent standard.
- **Default privacy settings:** The requirement of high privacy settings by default is an essential element of both design codes. However, the California AADC does not provide additional guidance on operationalizing this standard, and contains an exemption from the requirement not found in the UK AADC.
- **Age assurance:** While both design codes require a version of age assurance, the California AADC does not include risks to consider when balancing age estimation against data minimization.
- **DPIAs:** In contrast to the UK AADC's data protection impact assessments (DPIAs) requirement, the California AADC narrows the scope to risks of "material detriment," and requires a DPIA for any service, product, or feature, while the UK AADC requires a DPIA for a service.

As analyzed in FPF's policy brief, the California Age-Appropriate Design Code Act (California AADC) is a first-of-its-kind privacy by design law in the United States that will go into effect on July 1, 2024. The law regulates how children's data is processed and managed, and will have a broad impact on children's experience with online products and services. The California AADC draws inspiration from the United Kingdom's Age Appropriate Design Code (UK AADC).

Although the California legislature modeled its AADC after the UK AADC, there are significant distinctions between the two design codes. The analysis below provides a side-by-side comparison of the principles laid out in the UK AADC juxtaposed against the text of the California AADC. Understanding the requirements of both the UK and California AADC is useful because many businesses with a global presence will need to conform with both, and businesses who have not needed to conform with the UK AADC may nevertheless look to the Information Commissioner's Officer's (ICO) guidance for compliance until there is more clarity in California.

Key Distinctions in Regulatory Frameworks

It is important to understand the distinctions in the underlying regulatory frameworks when comparing the UK AADC to the California AADC, as this is one of the biggest distinctions between the two codes.

The UK AADC is a statutory code of practice prepared under the UK's General Data Protection Regulation (GDPR) that is intended to provide proper safeguards for children online.[1] The UK AADC language also refers to the certain standards in the European Union GDPR that have been adopted by the UK GDPR. A statutory code of practice is meant to give "guidance on good practice in the processing of personal data." This code is intended to help in complying with the principles and the legal obligations of the GDPR. Therefore, the UK AADC and the GDPR must be read together. Nonconformance with the standards of the UK AADC indicates that a covered entity is "likely to find it more difficult to demonstrate" that data processing complies with the GDPR. The ICO would consider the provisions of the UK AADC when considering questions of fairness, lawfulness, transparency, and accountability under the GDPR, and in use of enforcement powers.

In contrast, California's AADC is standalone legislation and will be independently enforced. The California AADC is intended to "further the purposes" of the California Consumer Privacy Act of 2018 (CCPA), but it does not rely on the enforcement mechanisms of the CCPA. Under the California AADC, the California Attorney General may seek an injunction or civil penalty against any business who violates its provisions. The California AADC is a novel approach to children's privacy in the US, and as businesses await any further guidance from the working group or possible rulemaking, it may be useful to understand the points of comparison and divergences from the UK AADC.

Legislative Considerations When Reading the UK AADC

The UK AADC is "rooted" in Article 3 of the United Nations Convention on the Rights of the Child (UNCRC). The UNCRC is an international treaty ratified by 195 countries that recognizes children's human rights. The UNCRC is ratified by the United Kingdom, but not by the United States. The ICO was required to consider the UNCRC when drafting the UK AADC. Therefore, the explanatory text of the UK AADC contains multiple references to the UNCRC that should be taken into account when looking at the relevant standards, most notably the "best interests of the child" standard.

The UK AADC provides 15 standards, along with a detailed description of each principle, and the relevant GDPR Articles and Recitals that the principle is derived from. It is necessary to consider each principle within the context of the relevant GDPR provisions, which are referenced within the UK AADC guidance, because the UK AADC is not independently enforceable. Our comparison below includes each of the 15 standards, numbered within parentheses, as well as the relevant GDPR provisions to illustrate the rationale and scope of the law. Guidelines of the European Data Protection Board (EDPB), an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, are also relevant since they provide clarifications and promote a common understanding of the GDPR.

[1] As explained in the ICO guidance on the UK AADC, the UK GDPR sits alongside an amended version of the Data Protection Act of 2018. The code is based on the provisions of the DPA 2018 and EU GDPR, but the key data protection principles, rights, and obligations underlying the code remain the same under UK GDPR.

Key Observations

- **Guidance and Tools for Compliance:** A consistent distinction from the UK AADC is that the California AADC in several instances does not define terms or provide additional guidance on compliance requirements. While the California AADC draws closely from the standards of the UK AADC, each UK standard is typically accompanied by explanations and examples.

- **"Best Interests of the Child":** The UK AADC implements the "best interests of the child" standard from the UNCRC. This standard is an embedded requirement for the design and development of services and the law emphasizes its importance throughout the UK AADC provisions. The US has not ratified the UNCRC and is thus not bound by its terms. However, the California AADC inserted a similar "best interests of children" standard in its exemption for adhering to the default privacy setting requirement, as well as in its legislative findings as a factor to consider when designing online services, products, and features. Without the foundation of the UNCRC, the standard implemented in the California AADC does not provide clear considerations for businesses in determining the "best interests of children."

- **Default Privacy Standards:** A key element of both the California AADC and UK AADC is the requirement that covered entities implement high privacy default settings. The UK AADC provides clear guidance about what "high" default privacy means, explaining that only the minimum amount of personal data should be collected and retained, children's data should not usually be shared, and geolocation services should be turned off. The California AADC, however, provides no further guidance to explain the "high level of privacy" required. The default privacy setting provision is further confused by the California AADC's exemption from the requirement if a covered entity can demonstrate a "compelling reason" that a different setting is "in the best interests of children," without further describing how the legislature understands those standards.

- **Age Assurance:** Estimating the age of users is required by both design codes. This provision raises concerns about the need to collect additional data from child users, creating more risks, to accurately estimate age. The UK AADC provides guidance on various appropriate measures that may be used to establish the age of users ("age assurance") while maintaining compliance with data protection obligations. Recognizing the potential for overcollection of data to identify age, the UK AADC clarifies that privacy by design solutions mitigate these risks. The California AADC requires covered entities to estimate the age of young users "with a reasonable level of certainty appropriate to the risks that arise from the data management practices," but there is no mention of what risks should be considered in balancing age estimation and appropriate protections. Additionally, the California AADC's legislative findings instruct businesses to design services based on a users' estimated age due to unique needs for listed age ranges. However, there is no guidance for businesses on how they should determine what is appropriate for each age range.

- **Data Protection Impact Assessments:** Both the UK AADC and California AADC require covered entities to conduct data protection impact assessments (DPIAs) to assess risks related to their data management practices and design features that are likely to be accessed by a child. However, the UK AADC requires an assessment of risks to rights and freedoms, while the California AADC narrows this consideration to risks of "material detriment." California AADC does not define "material detriment." Again, the UK AADC includes more guidance for covered entities and provides clearer considerations to include in their assessments. The California AADC requires a DPIA for any product, service, or feature, meaning that businesses may need to complete multiple assessments for a single product if there are multiple features "likely to be accessed by a child."

COVERED ENTITIES AND SCOPE

UK Age-Appropriate Design Code	California Age-Appropriate Design Code Act
The UK AADC applies to providers of information society services (ISS) who provide online products or services that **process personal data and are likely to be accessed by children**. The UK AADC states that "most online services are ISS, including apps, programs and many websites including search engines, social media platforms, online marketplaces, content streaming services (e.g. video, music or gaming services), online games, news or educational websites, and any websites offering other goods or services to users over the internet. This also includes connected toys and devices." **Child is anyone under 18**	The California AADC applies to a "business that provides an online service, product, or feature **likely to be accessed by children**." (Cal. Civ. Code § 1798.99.31). **Child is anyone under 18** (Cal. Civ. Code § 1798.99.30).
GDPR	**CCPA**
Article 4(25) references the EU Directive 2015/1535 definition of ISS, which is "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." **Article 4(7)** defines the controller and more clarifications are provided by the EDPB guidelines. CJEU case law along with the old Article 29 Working Party (A29WP) guidance (SNN & search engines) clarified that ISSPs may qualify as controllers. While the GDPR does not define "child," **Article 8** states that "the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 13 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years." Member States have used the possibility to deviate; 9 MSs apply the 16 years' age limit, 8 MSs apply the 13 years, 6 MSs apply the 14 years and 3 MSs apply the 15 years (an ISS has to determine the age of potential users depending on which MS they reside as stated by the **EDPB Guidelines**) **Recital 38:** "Children merit special protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child."	The CCPA defines a business as a legal entity operating for profit that collects consumers' personal information, determines processing of consumers' information, does business in California and meets one or more of the following requirements: (1) Gross 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)).

OBSERVATIONS: The UK AADC covers any provider of information society services, which it views as extending to most online services, including connected toys and other connected devices. While the California AADC also covers online services, the coverage is more tailored based on a provider's revenue and the extent to which they receive or sell consumer information.

ENFORCEMENT

UK Age-Appropriate Design Code	California Age-Appropriate Design Code Act
Tools to enforce include **assessment notices, warnings, reprimands, enforcement notices and penalty notices** (administrative fines). For serious breaches of the data protection principles, the ICO has the power to issue fines of up to €20 million or 4% of annual worldwide turnover, whichever is higher. **GDPR** **Article 58(2):** Provides for corrective powers like warnings, reprimands, fines, etc. **Article 82**: A data subject may request compensation for damages suffered. **Recital 85** gives several examples of such material or non-material damages: loss of control over personal data or limitation of rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. **Article 83**: Sets the general condition for imposing administrative fines. **Article 84**: Member states may create other penalties applicable to infringement.	Tools to enforce include **injunctions and civil penalties** of $2,500 per affected child for each negligent violation or $7,500 for each intentional violation. (Cal. Civ. Code § 1798.99.35 - Violations.)

OBSERVATIONS

The UK utilizes the ICO as its independent supervisory authority that monitors conformance with the UK AADC and would enforce any GDPR violations. In CA, the California AG may seek an injunction or civil penalty, but if within 90 days a business who is in substantial compliance with the requirements of the law fixes any noticed violation, provides a written statement, and takes measures to prevent future violations, the business will not be liable for a civil penalty. The GDPR, as the tool for ensuring conformance with the UK AADC, does not contain this cure period.

BEST INTERESTS OF THE CHILD

UK Age-Appropriate Design Code

Standard 1: Best interests of the child

The best interests of the child should be a **primary consideration when designing and developing online services** likely to be accessed by a child. This principle is directly taken from the UNCRC.

GDPR

Article 5(1)(a): Provides that "personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency)" and **Recital 38** states that "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences, and safeguards concerned and their rights in relation to the processing."

Article 6(1)(f): Data processing based on the grounds of a legitimate interest is possible unless the legitimate interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

California Age-Appropriate Design Code Act

The "best interests of the child" standard was **removed as a standalone requirement**. Instead, "best interest of children" is contained in the legislature findings (Cal. Civ. Code § 1798.99.29), and as an exception to requirements or prohibitions for:

- Configuring highest profile settings by default. (Cal. Civ. Code § 1798.99.31(a)(6)).
- Profiling. (Cal. Civ. Code § 1798.99.31(b)(2)).
- Collecting, selling, sharing, or retaining personal information. (Cal. Civ. Code § 1798.99.31(b)(3)).
- Using personal information for a purpose other than for the purpose it was collected. (Cal. Civ. Code § 1798.99.31(b)(4)).

OBSERVATIONS

The "best interests of the child" standard is a core principle of the UK AADC, which makes direct references to the UNCNC. While the California AADC mentions a similar, but not identical, "best interests of children" standard in the few places listed, there is no definition or guidance within the law. The law is also unclear on how businesses are to determine what is in the best interests of children, especially as a child is any individual under 18. Additionally, because the U.S. has not ratified the UNCRC, there is no established U.S. legal standard for "the best interest of the child" outside of the family law context.

DATA PROTECTION IMPACT ASSESSMENTS

UK Age-Appropriate Design Code

Standard 2: Data protection impact assessments

Undertake a DPIA to assess and mitigate risks to the rights and freedoms of children who are likely to access the service, which arise from data processing. **Take into account differing ages, capacities and development needs** and ensure that the DPIA builds in compliance with the code.

DPIAs must describe the nature, scope, context, and purposes for design. It must also **assess the risk of harm or damage whether physical, emotional, development, or material**, including:

- Physical Harm
- Online Grooming
- Social Anxiety/Self-Esteem Issues or Bullying
- Misinformation or undue restriction of information
- Encouraging excess risk taking
- Excessive screen time
- Economic exploitation

GDPR

Article 35(1): Processing likely to result in a high risk to the rights and freedoms of natural persons, requires a DPIA.

Article 35(3): Sets out examples of such high-risk processing.

Article 35(4): The Supervisory Authority is required to publish a list of processing operations that require a DPIA. The WP29 Guidelines list 9 indications to assess a high-risk processing. Data concerning vulnerable data subjects form such an indication.

Recital 75: Children may be indicated as vulnerable subjects due to the consideration that they are not able to knowingly and thoughtfully oppose or consent to the processing of their data.

California Age-Appropriate Design Code Act

Undertake a DPIA for any online service, product, or feature likely to be accessed by a child, **how it uses children's data, and the risks of "material detriment"** to children arising from data management practices of the business. (Cal. Civ. Code § 1798.99.31(a)(1)).

DPIAs shall address whether the design could:

- Harm children
- Lead to children experiencing or being targeted by harmful contacts
- Permit children to be subject to harmful conduct
- Expose children to exploitation by harmful contacts
- Harm children with its algorithms
- Harm children with its targeted advertising systems
- Harm children with incentive or engagement features
- Collect sensitive personal information

OBSERVATIONS

The UK AADC requires an assessment of risks to rights and freedoms, while the California AADC narrows this consideration to risks of "material detriment." The California AADC does not define "material detriment."

AGE ASSURANCE

UK Age-Appropriate Design Code	California Age-Appropriate Design Code Act
Standard 3: Age appropriate application Take a **risk-based approach to recognising the age of individual users** and ensure effective application of the standards in the code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from data processing, or instead apply the standards in the code to all users. **GDPR** **Recital 38:** "Children merit special protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child."	**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 apply the privacy and data protections afforded to children to all consumers. (Cal. Civ. Code § 1798.99.31(a)(5)).

OBSERVATIONS

While the California AADC's age estimation concept comes from the UK AADC's "age assurance," the UK AADC provides guidance and explanation as to how to comply, giving business various potential options to establish age while adhering to the other data protection principles. The California AADC adopted the UK AADC's age ranges, which the UK AADC includes for assessing risks of harmful effects to children. The California AADC does not indicate how to treat the different "age ranges" listed. The age ranges included in both codes are:

- **0-5 yrs**: Preliterate and Early Literacy
- **5-9 yrs**: Core Primary School Years
- **10-12 yrs**: Transition Years
- **3-15 yrs**: Early Teens
- **6-17 yrs**: Approaching Adulthood

TRANSPARENCY

UK Age-Appropriate Design Code	California Age-Appropriate Design Code Act
Standard 4: Transparency The privacy information provided to users, and other published terms, policies and community standards, **must be concise, prominent, and in clear language suited to the age of the child**. Provide additional specific '**bite-sized' explanations** about how the business uses personal data at the point that use is activated. **GDPR** **Recital 58:** Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand. **Article 12(1):** A controller should communicate information to data subjects (irrespective of their age) in a concise, transparent, intelligible and easily accessible form, using clear and plain language, noting that this obligation applies "in particular for any information addressed specifically to a child." The transparency principle is among the ones listed in **Article 5(1)(a)**. **Articles 13 and 14:** Set out specific obligations for controllers regarding the information that they are required to provide to data subjects when controllers process their personal data.	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. (Cal. Civ. Code § 1798.99.31(a)(7)).

OBSERVATIONS

The California AADC matches the "concise, prominent, and clear" language from the UK AADC that businesses must follow in disclosing privacy information, terms of services, policies, and community standards provided to users. The California AADC omits the UK AADC's requirement of providing "bite-sized" explanations when personal data is activated.

DETRIMENTAL USE OF DATA

UK Age-Appropriate Design Code	California Age-Appropriate Design Code Act
Standard 5: Detrimental use of data Do not use children's personal data in ways that **have been shown to be detrimental to their wellbeing, or that go against industry codes of practice**, other regulatory provisions, or Government advice. **GDPR** **Article 5(1)(a):** Includes the Fairness Principle and **Recital 2** underlines that "this Regulation is intended to contribute. . . to the well-being of natural persons." **Recital 75:** Risk to the rights and freedoms of natural persons, or varying likelihood and severity may result from personal data processing which could lead to physical, material, or non-material damage, in particular where personal data of vulnerable natural persons, in particular children, are processed.	Businesses shall not 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. (Cal. Civ. Code § 1798.99.31(b)(1)).

OBSERVATIONS

The UK standard prohibits processing children's data in ways that are "obviously, or have been shown to be" detrimental to health or wellbeing. The guidance provides examples of potentially relevant areas: marketing and behavioral ads, broadcasting, the press, online games, and user engagement strategies. The California AADC instead relies on a knowledge requirement of anything "materially detrimental."

POLICIES AND COMMUNITY STANDARDS

UK Age-Appropriate Design Code	California Age-Appropriate Design Code Act
Standard 6: Policies and community standards Uphold the business' own **published terms, policies and community standards** (including but not limited to privacy policies, age restriction, behaviour rules and content policies). **GDPR** **Article 5(1)(a):** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. **Article 5(1)(b):** Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. **Article 25(1)**: The controller shall implement the appropriate technical and organizational measures in order to ensure compliance with data protection principles.	Enforce published **terms, policies, and community standards** established by the business, including, but not limited to, privacy policies and those concerning children. (Cal. Civ. Code § 1798.99.31(a)(9)).

OBSERVATIONS

The California AADC does not provide any further explanation as to what classifies as adequate enforcement of policies or standards under its code. The UK AADC guidance states that "you need to use your privacy information to tell users what you will do with their personal data and why, and then make sure to follow through on that practice." The UK AADC also emphasizes that platforms must have adequate systems in place to properly uphold policies.

DEFAULT SETTINGS

UK Age-Appropriate Design Code	California Age-Appropriate Design Code Act
Standard 7: Default settings Settings must be **'high privacy' by default** unless a service can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child. **GDPR** **Article 25(2):** Implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. According to the **EDPB** Guidelines on Data Protection by Design & Default, "controllers should by default give data subjects an opportunity to intervene before personal data is made available on the open Internet. This is particularly important when it comes to children and vulnerable groups." There is also the recommendation that "Controllers, processors and producers, should consider their obligations to provide children under 18 and other vulnerable groups with specific protection in complying with DPbDD".	Configure all **default privacy settings** provided to children by the online service, product, or feature **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. (Cal. Civ. Code § 1798.99.31(a)(6)).

OBSERVATIONS

Both the California AADC and UK AADC use the standard of "high" privacy settings. The UK AADC says this means that "children's personal data is only visible or accessible to other users of the service if the child amends their settings to allow this.". While both codes allow for an exception, the "compelling reason" under the California AADC must be in the best interests of children rather than merely a consideration.

DATA MINIMIZATION

UK Age-Appropriate Design Code	California Age-Appropriate Design Code Act
Standard 8: Data minimisation **Collect and retain only the minimum amount of personal data needed** to provide the elements of the service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate. **Standard 9: Data sharing** **Do not disclose children's data** unless the service can demonstrate a compelling reason to do so, taking account of the best interests of the child. **Standard 14: Connected toys and devices** If a business provides a connected toy or device, include effective tools to enable conformance to the code. **GDPR** **Article 5(1)(c): "**Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (data minimization)." **Recital 57:** If personal data processed by a controller does not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of the GDPR. This requirement should be read in conjunction with the **EDPB** Guidelines. » With respect to verifying children's age, controllers are expected to make reasonable efforts for achieving such verification even though not explicitly required by the text of the GDPR. In any case, age verification should not lead to excessive data processing. » With regards to the authorisation of a holder of parental responsibility, the GDPR does not specify practical ways to gather the parent's consent and therefore the EDPB "recommends the adoption of a proportionate approach, . . . focusing on obtaining a limited amount of information, such as contact details of a parent or guardian."	A business **shall 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 as described in paragraphs (1) to (4), inclusive, of subdivision (a) of 1798.145, 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 likely to access the online service, product, or feature. (Cal. Civ. Code § 1798.99.31(b)(3)).

OBSERVATIONS

Both codes contain exceptions to data minimization requirements if a business demonstrates a "compelling reason" considering "the best interests of the child." The UK AADC provides an example of a compelling reason: sharing data for safeguarding purposes to prevent sexual exploitation and abuse online and to prevent/detect crimes against children like online grooming. The California AADC did not adopt the UK AADC's section on connected toys and devices, which requires that connected toys or devices that collect personal data must also conform to the standards of the code.

GEOLOCATION INFORMATION

UK Age-Appropriate Design Code	California Age-Appropriate Design Code Act
Standard 10: Geolocation **Geolocation options should be switched off by default**, unless a service can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child, and **provide an obvious sign for children** when location tracking is active. Options which make a child's location visible to others should default back to 'off' at the end of each session. **GDPR** **Article 5(1)(b):** The purpose limitation principle requires that personal data shall be collected for "specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes." **Article 5(1)(c): "**Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed."	A business shall not: (5) **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. (Cal. Civ. Code § 1798.99.31(b)(5)). (6) Collect any precise geolocation information of a child without **providing an obvious sign to the child** for the duration of that collection that precise geolocation information is being collected. (Cal. Civ. Code § 1798.99.31(b)(6)).

OBSERVATIONS

The California AADC closely mirrors the UK AADC's geolocation principle. The UK AADC provides an example of an exception: metrics needed to measure demand for regional services may be sufficiently un-intrusive to be warranted.

PARENTAL CONTROLS

UK Age-Appropriate Design Code	California Age-Appropriate Design Code Act
Standard 11: Parental controls If a service provides parental controls, **give the child user age appropriate information about those controls**. If the online service allows a parent or carer to monitor their child's online activity or track their location, **provide an obvious sign to the child when they are being monitored**. **GDPR** **Article 5(1)(a):** Provides that "personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency)" **Article 8:** The processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 13 years, such processing shall be lawful only if and to the extent that consent is given or author by the holder of parental responsibility over the child.	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**. (Cal. Civ. Code § 1798.99.31(a)(8)).

OBSERVATIONS

The California AADC mirrors the UK AADC's requirement to provide an obvious signal to the child when the child is being monitored by parents. However, the California AADC does not include any mentions of parental controls or providing age-appropriate information about parental controls. Additionally, the California AADC extends to *any* consumer monitoring of a child's online activity rather than solely by a parent or guardian.

PROFILING

UK Age-Appropriate Design Code	California Age-Appropriate Design Code Act
Standard 12: Profiling **Profiling should be 'off' by default,** unless a service can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child. Only allow profiling if appropriate measures are in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing). **GDPR** **Article 22:** General prohibition for automated decision making, including profiling, and certain exceptions to this rule. It does not include a distinction between adult and underaged data subjects. According to **Recital 71**, automated decision making should not apply to a child. However, the Recitals do not have a binding legal force. According to the WP29 guidelines on Automated Decision Making, given that the wording of the Recital is not reflected in the Article 22, "WP29 does not consider that this represents an absolute prohibition on this type of processing in relation to children. However, in the light of this recital, WP29 recommends that, as a rule, controllers should not rely upon the exceptions in Article 22(2) to justify it. There may nevertheless be some circumstances in which it is necessary for controllers to carry out solely automated decision-making, including profiling."	A business **shall not profile a child by default** unless both of the following criteria are met: (A) The business can demonstrate it has appropriate safeguards in place to protect children. (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)).

OBSERVATIONS

The UK AADC further explains that any exceptions to profiling will be narrow, and only apply when profiling is essential to the service. The ICO makes clear that any exceptions claiming behavioral advertising as a necessary feature, and not subject to being off by default, will be very rare. The definition of profiling in the California AADC mirrors that in the CCPA, which is subject to regulation from the California AG regarding access and opt-out rights. (Cal. Civ. Code § 1798.185(a)(16)).

NUDGE TECHNIQUES

UK Age-Appropriate Design Code	California Age-Appropriate Design Code Act
Standard 13: Nudge Techniques Do not use nudge techniques **to lead or encourage children to provide unnecessary personal data or turn off privacy protections**. **GDPR** According to the **EDPB** Guidelines on dark patterns, "regarding the data protection compliance of user interfaces of online applications within the social media sector, the data protection principles applicable are set out within **Article 5**. **Article 5(1)(a):** The principle of fair processing serves as a starting point to assess whether a design pattern actually constitutes a 'dark pattern.' Further principles playing a role in this assessment are those of transparency, data minimisation and accountability under **Article 5(1)(a)**, **Article 5(1)(c), Article 5(2)** as well as, in some cases, purpose limitation under **Article 5(1)(b)**. In other cases, the legal assessment is also based on conditions of consent under **Articles 4(11)** and **7** or other specific obligations, such as **Article 12**. Evidently, in the context of data subject rights, the third chapter of the GDPR also must be taken into account. Finally, the requirements of data protection by design and default under **Article 25** play a vital role, as applying them before launching an interface design would help social media providers avoid dark patterns in the first place."	A business shall not use **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)).

OBSERVATIONS

The UK AADC refers to nudge techniques, where the California AADC refers to "dark patterns," a term used in other California privacy legislation. The UK's nudge techniques principle makes no reference to the "materially detrimental" standard used in the California AADC.

ONLINE TOOLS

UK Age-Appropriate Design Code	California Age-Appropriate Design Code Act
Standard 15: Online tools Provide **prominent and accessible tools** to help children exercise their data protection rights and report concerns. **GDPR** **Article 17:** Provides the right to erasure. The right may be exercised when "the personal data has been collected in relation to the offer of information society services referred to in article 8.1. **Recital 65** further explains that the right "is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet" and that "the data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child." **Article 12(2):** The controller shall facilitate the exercise of data subject rights under Articles 15 to 22: » The right of access » The right to rectification » The right to erasure » The right to restrict processing » The right to data portability » The right to object » Rights in relation to automated decision making and profiling	Provide **prominent, accessible, and responsive tools** to help children, or if applicable their parents or guardians, exercise their privacy rights and report concerns. (Cal. Civ. Code § 1798.99.31(a)(10)).

OBSERVATIONS

While the UK AADC focuses on the child's ability to access these tools, including recommendations as to how to make them age appropriate by age range, the California AADC includes parents "if applicable." There is no further clarification or indication as to when parental access to tools would be applicable. Additionally, this principle of the UK AADC is meant to facilitate the ability of children to exercise multiple rights under the GDPR, but not all of these rights are contained within the California AADC.

FUTURE OF PRIVACY FORUM

About FPF //

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

Want to talk about privacy legislation?

Contact us at info@fpf.org, visit www.fpf.org, or follow us on Twitter: @futureofprivacy.

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