Safer by Design: How the CA Age Appropriate Design Code Would Change Children's Online Experiences

Companies Must Stop:

Using data about kids in anyway that harm them Kids' data is often used to develop features and algorithms that can harm them. The Code would stop companies using their data to, for example, train algorithms that serve them up pro-eating disorder or self- harm content.	**Tracking their locations** We wouldn't let strangers follow our kids around for no reason, so we're not sure why we let apps. The Code would stop companies tracking the precise locations of children unless it was essential to their service (like a map app).	**Collecting tracking location without making it clear** If an app does need to track a young person's location, like a map app, the Code would make sure that companies have to tell children when tracking is turned on. Simple.
Selling kids' data Let us count the number of steps you take each day so you can track your fitness! Secretly, we'll also sell this data on to advertisers, insurance companies or the highest bidder. The Code would prevent companies sharing or selling children's data unless it was essential to the service.	**Collecting personal data about kids they don't need (or if they're not sure if someone is a kid or not)** Many apps collect all sorts of information they don't need about kids, from data about who is in their phone book to what other apps they have. But each data point presents a privacy risk for young people. The Code would limit companies to only collecting the data they need.	**Profiling kids** Lots of companies profile children for unnecessary reasons, like to make advertising profiles. But profiling can harm kids. We've seen for example, social media companies profile kids as interested in drugs or alcohol. The Code would stop companies profiling children unless it was essential.
Using kids' data in ways that they didn't ask permission for Companies should only be allowed to use your data for the reasons you agreed to. For example, if you agreed to let them scan your phone book to 'find your friends' on an app, they should not be allowed to keep your friends phone numbers and sell them on to advertisers.	**Tricking them with dark patterns** CLICK HERE TO AGREE! (There's no 'decline' button) YOU'LL HAVE MORE FUN IF WE SCAN YOUR PHONE! (Or click 'No, I hate fun') Apps & websites shouldn't use tricky designs to trick young people into agreeing to collect data. The Code would stop that.	**Using data collected to estimate age for other purposes** Some websites & apps may collect data to better estimate the age of their users. This could help prevent 13 year olds from buying guns or pornography online. But if you collect that sort of data, you shouldn't be able to sell it, share it, or use it for any other purposes. The Code would ensure that.

Companies Must:

Do an assessment about how they use kids data, before they cause harm The Code would make companies do a simple risk assessment of the way they use kids data before they can cause harm. This is one way to make sure kids are 'safe by design', and identify and mitigate risks before harm happens.	**Set all default settings to the most private** Many platforms and services give people choices about how private they want their accounts to be. The Code would simply make sure that all new accounts start out on the 'most private' settings, and users can change them later if they want to. This is about 'privacy by design'.	**Make it easy for kids to report privacy concerns** If something goes wrong, it's got to be easy for parents and kids to seek help if their privacy is violated. The Code asks companies to make it easy to report a concern, and for a timely and effective support process to be in place.
Let kids know when they are being monitored or tracked Many apps & websites allow parents and guardians to track or monitor children's use to ensure they are safe. The Code calls for transparency around this, and to let kids know when family apps are tracking their location or when parents have read messages. Transparency helps young people to develop responsibility.	**Live up to your policies and terms & conditions** Many digital services already have good policies and guidelines about what sort of content they do or do not allow on their platforms. But too often, these policies are not enforced and companies do not live up to what they say. This makes choosing the right service for kids hard, as platforms often don't do what they say. The Code has a simple requirement: you must enforce your terms & conditions.	**Provide all privacy notices in clear language that young users can understand** Have you managed to find the five hours it would take to read all of an app's policies? Have you got the legal degree you might need to understand it? No? Well, maybe the solution is simple. The Code says that companies should have to present their privacy notices and all terms and conditions in simple language we can all understand.
Reasonably establish the age of your users, in a way that matches the risks of your service **(or reduce the risks and maximise privacy for all consumers)** Being reasonably sure of the age of a user is not the same as confirming the identity of the user. The Code simply states that if you're going to do risky things with data, like sell sensitive biometric data and live location data to the highest bidder, you've got to be completely sure that this isn't kids data. The Code ensures that companies need to know who is and who is not a kid, in privacy preserving ways proportionate to the risks inherent in the design choices the company takes. A company that poses no risk would not need to implement age verification.		

How Children will Experience the Code:

1. Geolocation tracking will be turned off so companies don't know kids' every move

Children and young people's live location data is routinely tracked by apps and products that don't really need it. Data can be valuable, so many companies collect it and use it by default. But collecting geolocation data creates real privacy risks, and sometimes safety risks too.

For example, right now in California, because Snapchat is allowed to collect Geolocation data they use it to populate a feature called Snapmaps. If any users, young or old, looks at a Snapmap of a local high school, they can see videos and photos posted by students. We wouldn't allow strangers to wander through school campuses in person, so we probably shouldn't let them take digital walking tours either.

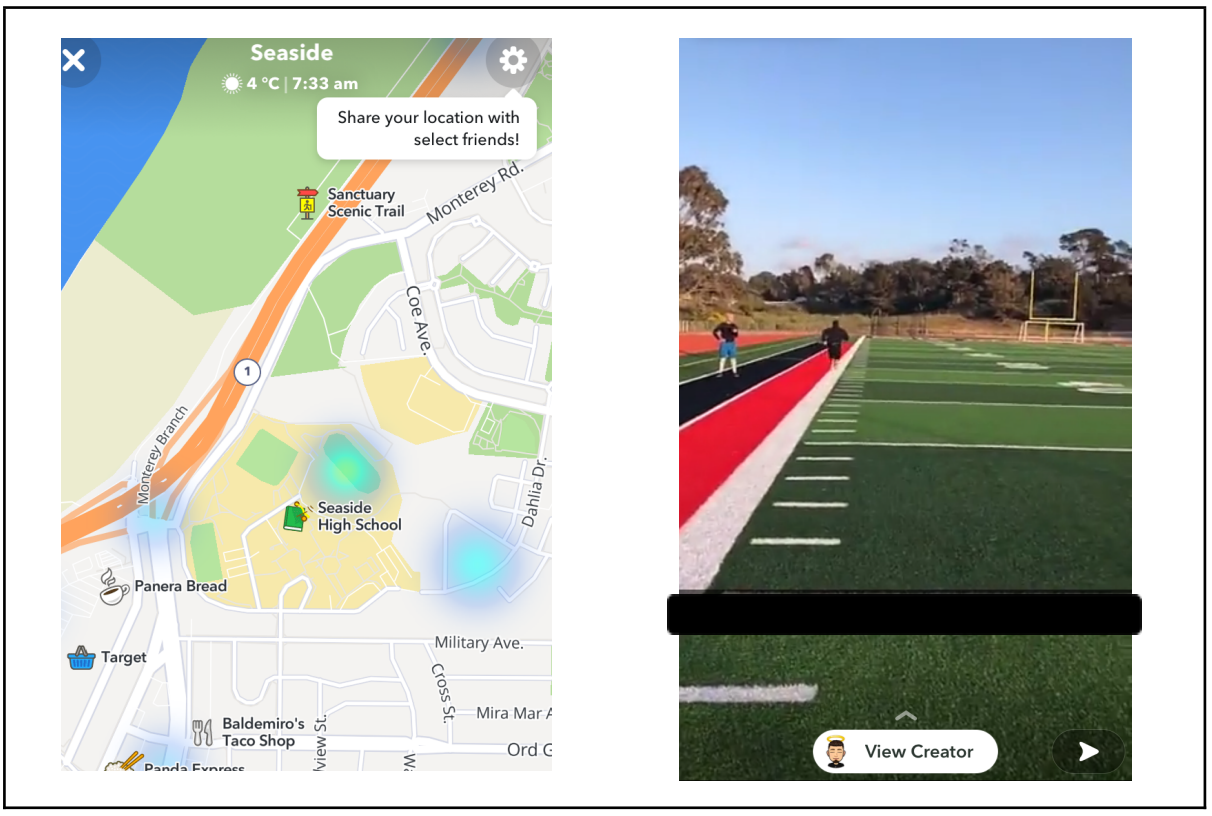


Figure 1: A Snapmap of a Califronian high school. The cyan dot over the school gates is a heat map, telling users that there's a lot of videos and content available to be seen here. When you click on it, you see pictures and videos from inside the school, with links to 'view the creators' (students) who posted them. We have included a nondescript, non-identifiable image to demonstrate this.

(Section of AB2273 that addresses this: 1798.99.31(b)6. *A business shall not collect any precise geolocation information by default, unless the business can demonstrate a compelling reason that doing so would be in the best interests of the child)*

2. Their social media accounts will be set to private by default

Many platforms allow users to have 'private' accounts with limited visibility or 'public' accounts which are searchable and widely promoted. Private accounts offer more privacy to younger users as well as more safety, by limiting contact with strangers. When a young person creates a new account on a social media platform, the platform has a choice about whether they should default this account to public, to private, or prompt the young person to choose. Upcoming research[1] shows that in the US both Instagram & TikTok by default set the accounts of 17 year olds to public. In the UK which already has a similar design Code in place, and the EU where one is being drafted, the accounts of 17 year olds are by default set to private or they are nudged to select private accounts.

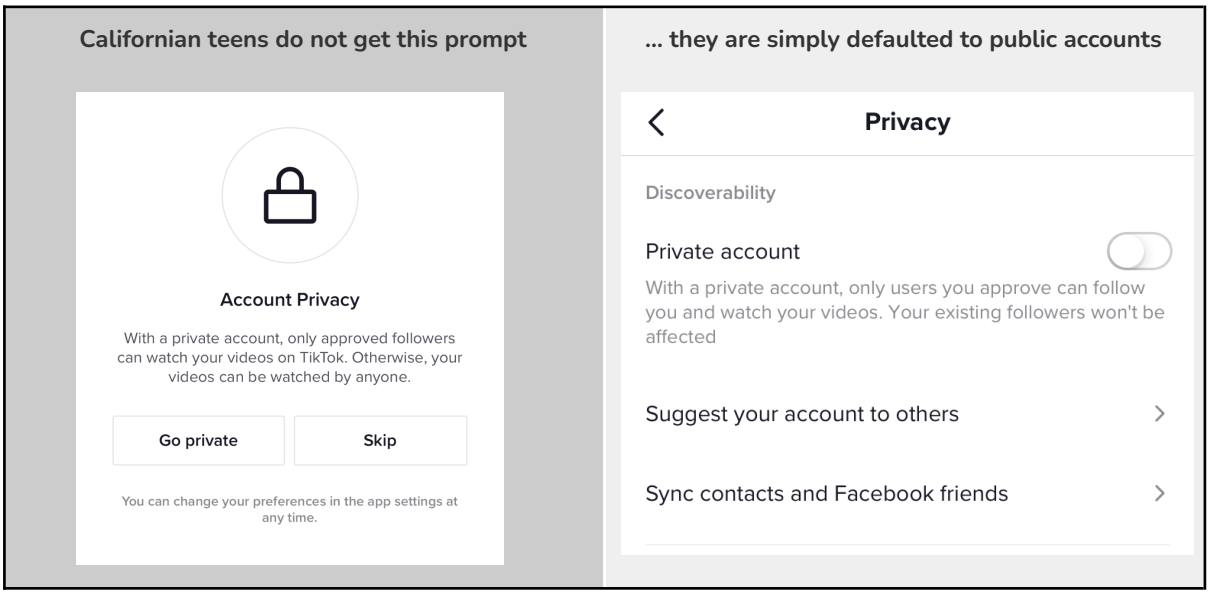


Figure 2: The prompt 17 year old British young people receive to turn their accounts private on TikTok (left). US accounts simply default to public accounts (right)

(Section 1798.99.31(a)4. *Maintain the highest level of privacy possible for children by default, including, but not limited to, disabling profiling, unless the business can demonstrate a compelling reason that a different default setting is in the best interests of children likely to access that good, service, or product feature).*

[1] Fairplay *et al* (forthcoming) Global Platforms, Partial Protections: Design Discriminations on Social Media Platforms

3. There won't see deceptive design that erodes their privacy

Lots of apps use sneaky language of design to trick young people into 'agreeing' to more data collection. From prompts telling kids that 'this app is more fun if you connect with friends, so give us access to your phone book', to navigation options that make the yes button big and shiny while hiding the no button in invisible grey in the corner … companies unleash years of UX research to erode young people's privacy. Upcoming research from the University of Michigan[2] describes this as a form of design abuse.

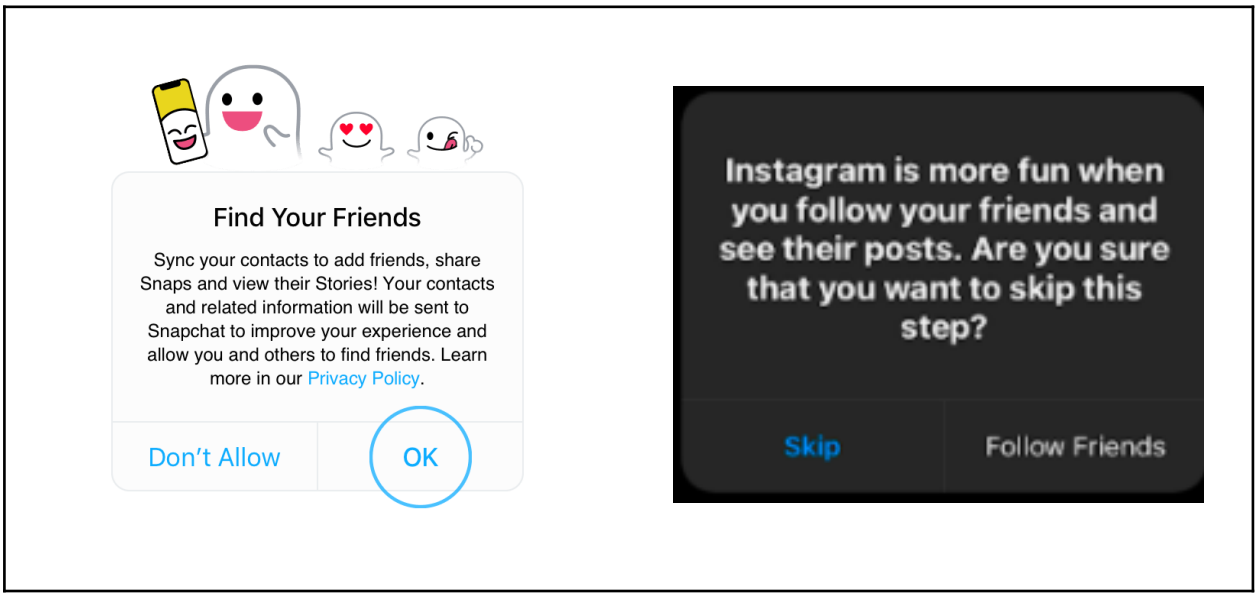


Figure 3: Screens shown to young users when joining Snapchat (left) and Instagram (right) that encourage young users to allow the platforms to scan their address books. If you initially select 'skip' on Instagram, a warning comes up to nudge you to reconsider; it's more 'fun' if you allow Instagram to collect this additional data. They also don't provide a 'no' button, just a 'skip' button

(Section 1798.99.31(b)9. *A company shall not use dark patterns or other techniques to lead or encourage consumers to provide personal information beyond what is necessary to provide that good, service, or product feature, to forego privacy protections, or to otherwise take any action that is demonstrably harmful to the consumer's physical health, mental health, or well-being*

[2] Radesky, J *et al* (forthcoming) 'Design Abuses in Apps'

4. Companies won't be collecting unnecessary data about them

Apps and websites often track young people across the internet., even apps for toddlers. Looking at the top ten most downloaded apps for under 5 year olds on iPads in April revealed the amount of tracking. The top ten free apps had on average 3.6 different tracking codes enabled, ranging from two to 10 trackers. The top paid for apps had 2.6 different tracking codes, ranging from none to 13. Trackers are pieces of code that 'track' how people use a service, what ads they click on and often where they go next. Many collect location and other personal data, and are often used to profile users for advertising.

Figure 4: The number of tracking codes enabled on one of the most downloaded apps in April 2022 in the USA for the under 5s[3].

(Section 1798.99.31(b)2: *A company shall not collect & retain any personal information that is not necessary to provide a good, service, or product feature with which a child is actively & knowingly engaged)*

5. They won't be profiled based on what they do or share online

Lastly, the Code could protect children against future abuses of their data that we can't yet foresee. For example, lots of sensitive data, such as biometric data, is collected about children from Fitbits that monitor activity levels, to wellness apps that collect data about mental health to wearables for newborns that have heartbeat monitors installed. Left unregulated, this sensitive data could be used to limit children's future life chances and discriminate against them. For example, health information could be sold to health insurance companies and data about heart murmurs in babies or mental health issues as teenagers could be used to hike up insurance premiums in your 50s. These risks will only increase as the use of algorithms to automate decision making increases. As Unicef[4] outlines:

> *Algorithms tend to reproduce patterns of bias and historical discrimination found in the data used to train them. The use of machine learning tools to assess student performance has resulted in already marginalized children being further targeted for disciplinary actions and labelled pre-emptively as more likely to engage in criminal or other anti-social behaviours. Scores used in criminal risk assessments in the United States have habitually recommended harsher sentences, higher bonds, and lower likelihoods of parole for black people, including black children and youth, than for white people despite these practices proving to be both unfair and unjustified in comparative studies of actual recidivism. Bias and mistakes that lead to the exclusion of children or their families from cash transfers, scholarships, housing, health benefits or other aid and entitlements can have dire consequences.*

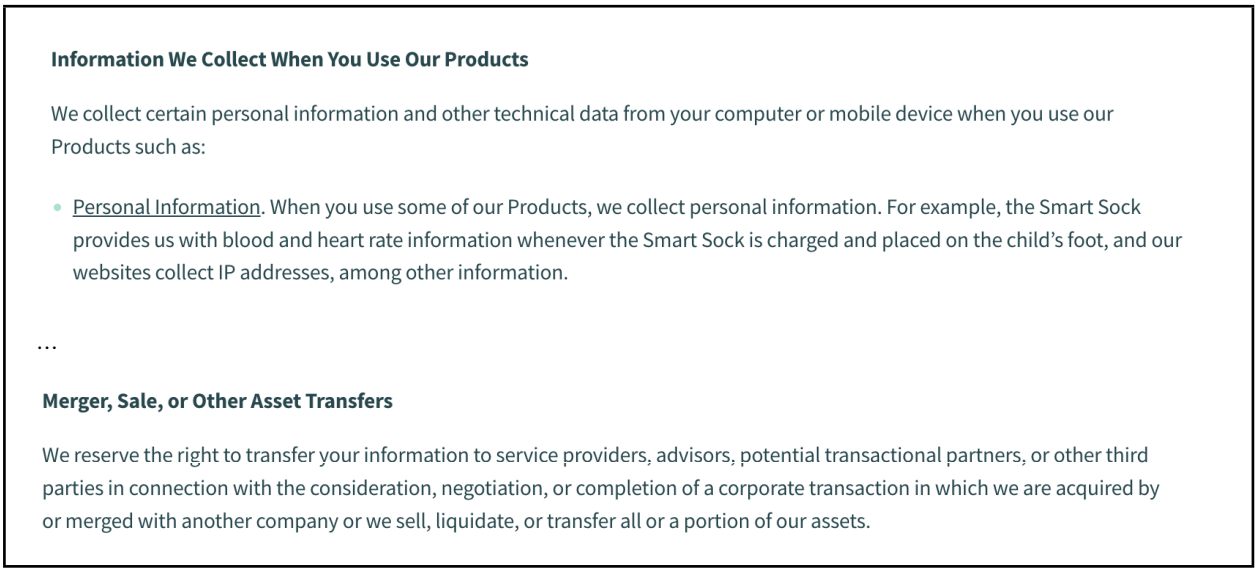
[3] With thanks to Exodus Privacy

[4] Unicef 2020 *The Case for Better Governance of Children's Data: A Manifesto* www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf

Globally, there have been many examples where children's data has already been used to reduce their life chances and discriminate in ways that were not anticipated. For example:

- In 2020, in the UK a 'mutant algorithm' was deployed to downgrade the high school grades of school leavers from low income areas[5]
- Between 2017 and 2020, the Australian Government uses an algorithm to automate tax and benefit debt assessment and recovery that wrongly 'reclaimed' $1.2bn from Australian families[6]
- Between 2013 and 2019 the Dutch government used data to racially profile families and wrongly accused 26,000 families of falsely claiming childcare benefits. The entire Cabinet eventually resigned[7]

Currently, lots of sensitive personal data is being collected about Californian children, without adequate safeguards to protect against future abuses or descrimination, including biometric data.



Information We Collect When You Use Our Products

We collect certain personal information and other technical data from your computer or mobile device when you use our Products such as:

- Personal Information. When you use some of our Products, we collect personal information. For example, the Smart Sock provides us with blood and heart rate information whenever the Smart Sock is charged and placed on the child's foot, and our websites collect IP addresses, among other information.

...

Merger, Sale, or Other Asset Transfers

We reserve the right to transfer your information to service providers, advisors, potential transactional partners, or other third parties in connection with the consideration, negotiation, or completion of a corporate transaction in which we are acquired by or merged with another company or we sell, liquidate, or transfer all or a portion of our assets.

Figure 5: The US privacy policy of a wearable baby device that collects heart rates and oxygen levels. The company outlines their ability to collect personal information, such as heart rates, and also their ability to sell or transfer this data as part of an asset transfer. No safeguards nor provisions are included to ensure the 'safe' user of this data if it is sold on.

(Section 1798.99.31 (b) 5 *A business shall not* disclose *the personal information of any child unless the business can demonstrate a compelling reason that disclosure of that personal information is in the best interests of the child.* Section 1798.99.31 (b) 1: *A business shall not use the personal information of any child in a way that is demonstrably harmful to the physical health, mental health, or well-being of a child*).

[5] Sean Coughlan 2020 'A Levels and GCSEs: Boris Johnson blames mutant algorithm for exam fiasco' www.bbc.com/news/education-53923279

[6] Rebecca Turner 2021 'Robodebt Condemned' *ABC* www.abc.net.au/news/2021-06-11/robodebt-condemned-by-federal-court-judge-as-shameful-chapter/10020767

[7] Amaro, Silvia 2021 'Dutch government resigns after childcare benefits scandal'. *CNBC* *www.cnbc.com/2021/01/15/dutch-government-resigns-after-childcare-benefits-scandal-.html*