Comments to the California Privacy Protection Agency

Introduction

Common Sense Media (Common Sense) and Privacy Rights Clearinghouse are pleased to submit these comments in response to the California Privacy Protection Agency (CPPA)'s invitation for preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020 (CPRA). Common Sense is an independent, nonpartisan voice for children that champions policy solutions that puts children--all those under 18--first and works to ensure that they can thrive in the 21st century. Privacy Rights Clearinghouse is a nonprofit organization dedicated to improving privacy for all by empowering individuals and advocating for positive change.

Question 1: Processing that Presents a Significant Risk to Consumers' Privacy or Security: Cybersecurity Audits and Risk Assessments Performed by Businesses

1. *Processing Children's Personal Information Presents a Significant Risk to Consumers' Privacy and Security That Should Require Businesses to Regularly Submit Risk Assessments*

Processing personal information of children and teenagers poses a significant risk to consumers' privacy and security, and businesses that process such information must be subject to the CPRA's requirement to conduct risk assessments. Children and teens spend increasing amounts of time online and are especially susceptible to privacy harms because their brains are still developing and they do not fully comprehend the consequences of sharing or the nature of advertising. Privacy policies and terms of service are insufficient to protect children, who can be easily exploited and manipulated and suffer behavioral, social, emotional, and physical harms. Risk assessments are therefore critical.

Children across all age groups are spending more time on devices and online than ever before. According to Common Sense research, even before the pandemic, children from birth to age 8 in the United States were using about two and a half hours of screen media per day, while 8- to 12-year-olds used just under five hours' worth, and teens used just under seven and a half hours.[1] These numbers do not include the time spent using screens for school or homework. Children in lower-income households also spend an average of nearly two hours a day more with screen media than those in higher-income homes. Similar patterns were found in Latino and Black children in comparison to white children. With education largely shifting online in 2020, kids also experienced a sizable 69 percent increase in the amount of time they spent

[1] The Common Sense Census: Media use by kids age zero to eight, 2020. San Francisco, CA: Common Sense Media.

using a screen for education, particularly 5- to 10-year old's.[2] While many children have returned to the classroom, reliance on technological tools is expected to continue.

The increasing presence of kids and teens online raises concerns for many reasons.[3] Young children and teens are prone to oversharing,[4] and because their brains are still developing, they have also been shown to not understand the consequences of their sharing.[5] They believe that the information they share remains on their device, or within an app or game, and that deleting the app or information within an app will delete it from the internet. They also do not understand that an app may gather information about them from sources outside the app.[6]

Children also have difficulty identifying advertising. More than half of thousands of free children's apps may serve kids ads that violate the Children's Online Privacy Protection Act (COPPA).[7] Yet research shows that children under the age of eight cannot comprehend the persuasive intent of advertising and are prone to accepting advertiser messages as truthful, accurate, and unbiased.[8] Over 75 percent of kids aged 8 to 11 cannot distinguish advertising from other content.[9] Even older children still lack the digital skills and critical ability to assess the safety of content they encounter online.[10] Privacy also exacerbates equity issues, as shown through findings that children with low socioeconomic status were more likely to play games collecting and sharing information for advertisements.[11]

Companies can exert influence over children through exploiting their susceptibility to coerce them into making choices they would not otherwise make, such as through behavioral targeted advertising. Misuse and the inadvertent disclosure of a child's personal information can lead to a wide range of behavioral, social, emotional, and physical risks, which are detailed extensively

---

[2] Ryan Tuchow, Kid device usage changing as a result of the pandemic, Kidscreen, (Feb. 19, 2021).
[3] Testimony of Ariel Fox Johnson Before the United States House of Representatives Committee on Energy and Commerce, Common Sense (March 11, 2021).
[4] Who Knows What About Me?, Children's Commissioner, (Nov. 8, 2018). The UK Children's Commissioner found that, pre-pandemic, children posted an average of 26 times a day to social media. By age 18, they average a total of 70,000 posts.
[5] Children may not understand what is going on, whereas teens may have a slightly better sense but be more likely to partake in risky behavior.; *see* Adriana Galvan et al., *Earlier Development of the Accumbens Relative to Orbitofrontal Cortex Might Underlie Risk-Taking Behavior in Adolescents*, 26 Journal of Neuroscience 25 (2006) (teens' brain development can bias them towards risky behaviors).
[6] Anonymous Author(s). 2021. "They See You're a Girl if You Pick a Pink Robot with a Skirt": How Children Conceptualize Data Processing and Digital Privacy Risks. In CHI '21: ACM CHI Conference on Human Factors in Computing Systems, May 8–13, 2021, Yokohama, Japan. ACM, New York, NY, US.
[7] Reyes et. al, "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. Proceedings on Privacy Enhancing Technologies, (2018).
[8] American Psychological Association. *Advertising leads to unhealthy habits in children; says APA task force*. [Press release] (Feb. 23, 2004).
[9] Common Sense Media, Privacy Matters: Protecting Digital Privacy for Parents and Kids, (2018).
[10] Nyst, Carly. (2017). *Privacy, protection of personal information and reputation*. Retrieved from UNICEF website: https://www.unicef. org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf.
[11] Zhao F, Egelman S, Weeks HM, Kaciroti N, Miller AL, Radesky JS. Data collection practices of mobile applications played by preschool-aged children. *JAMA Pediatrics*, accepted for publication.

in Common Sense's report Privacy Risks & Harms.[12] Children can experience cyberbullying, radicalization, substance abuse, limited educational opportunities, self-harm, contact from strangers, identity theft and increased parent-child conflict. These risks can be magnified for children who are already in more vulnerable groups.[13]

Privacy policies and terms of services alone cannot be relied upon to notify children and their parents of the implications of sharing information online and to obtain consent to collect and share their information. Even older and literate children struggle to understand privacy policies, which are often long and full of legal jargon. Only 17 percent of teens and 36 percent of parents say they read the terms of service "almost all the time."[14] Although parents are talking to their children more than ever about privacy,[15] the onus should not only be on parents to keep their children safe online. Even with consumers' perfect understanding of privacy policies, businesses can still misuse and exploit personal information collected about children.

Defining all children's personal information and data as information that presents a "significant risk to consumers' privacy or security," which would require businesses to submit regular risk assessments to the Agency regarding their processing activities, would be a step in the right direction to addressing the above discussed harms.

2. *Because Children's Personal Information Poses a Significant Processing Risk, Businesses Must Perform Risk Assessments that Consider the Purposes, Necessity, and Potential Harms of Such Processing in Early Stages of Product Development*

In conducting risk assessments, businesses should build them in at the start of their design processes and regularly thereafter. Businesses must consider the purpose and necessity of their processing--specifically whether it is needed for the product to work; the potential harms to children of such processing; and what mitigation measures are available.

Businesses should conduct risk assessments both early in the product or platform development stage and regularly after deployment. Platforms often engage in adult-centric design practices instead of taking into account the developmental needs of children when designing their products and features. Research has shown that platforms are often engaged in manipulative design practices that exploit children's developmental vulnerabilities.[16] By requiring risk assessments during the early product development stages, products targeted at children or often used by children can be designed with their safety and privacy in mind. This would also

[12] Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2019). Privacy risks and harms. San Francisco, CA: Common Sense Media.
[13] This includes children from poor households, children in communities with a limited understanding of different forms of sexual abuse and child exploitation, children who are out of school, children with disabilities, children who suffer from depression or other mental health problems, and children from marginalized groups. Nyst at 81.
[14] Common Sense Media, Privacy Matters: Protecting Digital Privacy for Parents and Kids, (2018).
[15] *Ibid*
[16] Letter from Common Sense and Dr. Jenny Radesky on Article 26 of the Digital Services Act (June 7, 2021).

save business resources, preventing a business from needing to make major overhauls after it has already developed, tested, or launched its product for public use and avoid preventable harms from the start.

Regular risk assessments after product deployment are also necessary to ensure businesses are continually operating with children in mind and assessing their data collection practices so that they do not begin collecting more information than is strictly necessary. Risk assessments should be conducted whenever a business adopts new technology or features, or wants to collect additional information, or on an annual or bi-annual basis.

Given the unique developmental stages and vulnerabilities of children, the risks of any data collection of children that is not necessary for the functioning of a product should be treated as outweighing the benefits. Common Sense supports the prohibition of behavioral targeted advertising to children altogether.[17] Businesses should perform risk assessments under the assumption that all information collected about children is sensitive personal information, and carefully scrutinize the implications of any data collection and processing.

The UK Age Appropriate Design Code, which went into enforcement effect in September 2021, also requires businesses conduct data protection impact assessments,[18] and we propose the law should be used as a model for what businesses should cover in these risk assessments submitted to the Agency. The assessments should have a detailed description of the nature, scope, context, and purposes of the processing. This includes information about whether the product or service is designed for children or whether children are likely to access the service, the age range of those children, any plans for establishing the age of those children or any parental controls, the intended benefits to children, the commercial interests of the business for the processing, and whether any profiling or automated decision making is involved. Also, in line with the Code, the assessment should assess the necessity of the processing, the proportionality of the benefits with its risks to children, and whether it complies with the CPRA, COPPA, and any other applicable laws.

With that information, the assessment must carefully consider any harm or damage the data processing may inflict on a child's physical, emotional, developmental, or social health. In particular, businesses should assess whether the processing may cause or lead to an increased risk of physical harm, sexual exploitation, social anxiety, self-esteem issues, depression, bullying, peer pressure, or compulsive use.

Finally, the assessment should identify measures to mitigate those risks and its plans for adopting them. Mitigation measures can include imposing new safeguards or eliminating a

[17] Testimony of Ariel Fox Johnson Before the United States House of Representatives Committee on Energy and Commerce, Common Sense (March 11, 2021).
[18] Alyona Eidinger, What is the Age Appropriate Design Code?, Common Sense Media, (Jan. 20, 2021); Information Commissioner's Office, Age Appropriate Design: A Code of Practice for Online Services, (Sept. 2, 2020).

specific feature or collection of specific data altogether. If the assessment finds that the risks posed by processing cannot be mitigated, businesses should cease processing the data.

By requiring risk assessments that detail data processing activities, assess the necessity and potential harms of processing, and propose any mitigation measures that can be implemented, businesses will be more transparent and can be held accountable for its data processing of children.

The CPPA should require that these risk assessments be disclosed to them, the Attorney General's office, and any other applicable regulatory or enforcement agencies for the particular business. To the extent doing so would further privacy interests, the agency may choose to disclose information from the reports at its own discretion, while keeping any trade secrets confidential and redacted. This will help further promote accountability and transparency among businesses.

Question 5: Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information

1. *The Use of Sensitive Information Should Be Limited Only to What is "Necessary to Perform the Service"*

All data about children under 18 is sensitive information, and thus businesses should only use this sensitive information when it is strictly necessary to perform the service it is offering to consumers. This is in line with already existing requirements under the Children's Online Privacy Protection Act for children under 13, along with international best practices such as the UK's Age Appropriate Design Code. This would be stricter than the current right consumers have under the CPRA, but is necessary to best protect children and make their best interests the priority instead of a business' commercial interests. Businesses should also change their assumptions about the reasonable expectations of consumers to better reflect reality and research that has found consumers are concerned about targeted advertising and the privacy concerns it poses.

The CPRA states that "a consumer shall have the right, at any time, to direct a business that collects sensitive information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services to perform the services." Under prohibitions dating back to the CCPA, the rules protecting children under 16 are default protected (no sale unless opt-in), and the most privacy protective way to read the CPRA is if that framework was extended to children under 16's for sensitive information as well. This is consistent with the CPRA's preamble which notes that "Children are particularly vulnerable from a negotiating perspective with respect to their privacy rights." The default should be that businesses can only use children's sensitive information for purposes that are strictly necessary to operate its service. This would best protect young people because it would mandate a default framework that puts children's privacy and security above minor commercial benefits a business may get.

The CPPA should also reconsider what an average consumer who requests a business to provide a good or service reasonably expects when evaluating whether a business is using sensitive information for necessary purposes. Businesses should not reasonably expect that consumers expect targeted advertising. Instead, businesses should expect that consumers would prefer other non-intrusive types of advertising that do not rely on collecting data about consumers to generate it such as contextual advertising, in which ads are displayed based on a website's content.

There are studies that would support this reasonable expectation. A study found that college students perceived the risk of targeted advertising to be higher than the benefits, which drives them to perceive more privacy concerns and avoid the advertising.[19] A cybersecurity survey found that just 17 percent of respondents across the United States, France, Germany, and the United Kingdom viewed tailored advertisements as ethical.[20] Most relevant, a survey has shown that 82 percent of parents and 68 percent of teens are concerned about how social networking sites are using their data to allow advertisers to target them with ads.[21] With children, teens, and their parents voicing so much concern about the use of their data for targeted advertising in conjunction with their discussed developmental vulnerabilities, there is compelling reason to revise what businesses consider these groups' reasonable expectations.

Question 6: Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information

1. *All Children's Data Should be Treated as Sensitive Personal Information Subject to the Right to Have Limited Use and Disclosure*

The term "sensitive personal information" should be interpreted as broadly as possible, particularly when it comes to children's data. Even data that may not be considered sensitive because it is deemed "collected or processed without the purpose of inferring characteristics about a consumer" can be used to make sensitive inferences. For example, cell tower location data indicating where a phone stays overnight could be used to infer a couple is getting a divorce,[22] and a business could use a person's shopping history to infer she is pregnant.[23] As a result, consumers must have the right to limit the use and disclosure of broadly defined sensitive personal information. There is no circumstance in which it is logical for a business to stop a consumer from exercising this right when it involves information that has already been categorized as sensitive.

---

[19] Business News Daily Editor, *Invasion of Privacy: What Consumers Think of Personalized Online Ads*, Business News Daily (Feb. 21, 2020), https://www.businessnewsdaily.com/4632-online-shoppers-personal-ads.html.

[20] RSA, *The Dark Side of Customer Data* (Feb. 6, 2019), https://www.rsa.com/en-us/company/news/the-dark-side-of-customer-data.

[21] Common Sense Media, Privacy Matters: Protecting Digital Privacy for Parents and Kids, (2018).

[22] Diane L. Danois, *Cohabitation, the Termination of Alimony, and Cell Phones*, The Huffington Post (June 11, 2013).

[23] Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, Forbes (Feb. 16, 2012).

2. No Use or Disclosure of Sensitive Personal Information Should be Permissible

No use or disclosure of a consumer's sensitive personal information by businesses should be permissible in spite of a consumer's direction to limit the use or disclosure of it. This is contrary to the purpose and intent of the CPRA, which a majority of Californians voted for in order to expand privacy rights. The consumers' rights under the CPRA should always take priority, and businesses should not be permitted to override a consumer's decision to exercise her right to limit the use or disclosure of her data in any circumstance. Businesses should not ever aim to use or disclose any more sensitive personal information than is strictly necessary.

Question 8j: "Dark Patterns" Should be Defined to Include Manipulative Design Features That Encourage Children to Give Up Personal Information

Dark patterns can cover a wide range of design choices that benefit an online service by pushing users to make potentially harmful choices that they would not otherwise make. The definition of "dark patterns," which would be better referred to as "manipulative design," should be drafted as broadly as possible and include at least design features that encourage children to give up personal information.

In a notable paper in the area, dark patterns were defined as "user interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions."[24] However, dark patterns include many types of practices and features. Researchers have found at least one dark pattern in 95 percent of apps in a study of 240 popular apps.[25] The definition the CPPA adopts should be as broad as possible to include the many ways dark patterns can take form.

Firstly, the term "manipulative design" should be adopted in place of "dark patterns" in CPPA regulations (recognizing the text of the CPRA refers to "dark patterns"). Evolving scholarship highlights how the term "dark patterns" perpetuates implicit racial biases because it is part of a dualism that sees darkness as inherently bad and light as good and thus should be updated.[26] The term "manipulative design" is also more informative and better acknowledges how businesses are essentially tricking consumers into making certain choices they would not make in the absence of the feature -- whether they mean to or not. Common Sense has shifted to using the term "manipulative design" recently, and will officially adopt the term in future content and filings in place of "dark patterns."

---

[24] Mathur et. al, "Dark Patterns at Scale: Findings From a Crawl of 11K Shopping Websites," Proceedings of the ACM on Human-Computer Interaction (2019).
[25] Linda Di Geronimo et. al, "UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception," Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (2020).
[26] Kat Zhou, FTC Dark Patterns Workshop Transcript, Federal Trade Commision (April 29, 2021) at 15; Kate Conger, "Master," "Slave' and the Fight Over Offensive Terms in Computing," N.Y. Times (Apr. 13, 2021).

In particular, the definition of manipulative design should include design features that encourage children to give up more personal information than necessary or than they may freely wish to.

Apps often encourage children to disclose personal information to play a game or participate in certain parts of it, interfering with promises companies set out in privacy policies.[27] A third of 135 Android apps reviewed in a 2018 study that were marketed to or played by children prompted players to rate the app on the Google Play store, and 14 percent prompted players to share information on social media.[28] The information shared often results in children unknowingly agreeing to provide the company with wide permissions to extract information about social media contacts, enabling companies to collect even more data. Additionally, a study found that almost half of 153 apps in Google Play's "Designed for Families" category transmitted advertising identifiers.[29] Multiplayer games also tend to use default settings that reveal the most personal information, which is particularly harmful for children who are unlikely to change or know how to change the settings.[30] The employment of manipulative design features trap users into data collection, making people lose the ability to make truly informed decisions.[31]

A broad definition of "dark patterns" or "manipulative design" like the one proposed here would put businesses on alert to deter them from engaging in dark patterns and allow parents to better understand what can be considered a "dark pattern" that they should watch out for.

Conclusion

Common Sense appreciates the CPPA's work on this rulemaking and urges the Agency to take the steps recommended in these comments to ensure that children and teens' privacy rights are protected.

Respectfully submitted,
Ariel Fox Johnson, Senior Counsel, Global Policy
Irene Ly, Policy Counsel
Common Sense

---

[27] Johanna Gunawan, "Right at the Source: Privacy Manipulative Design in User Interfaces," Common Sense Media (Oct. 13, 2021).

[28] Meyer M, Adkins V, Yuan N, Weeks HM, Chang YJ, Radesky J, *Advertising in Young Children's Apps: A Content Analysis*, J. Dev. Behav. Pediatr. (2019).

[29] Fangwei Zhao, et al, Data Collection Practices of Mobile Applications Played by Preschool-Aged Children, JAMA Pediatrics (Sept. 8, 2020), https://jamanetwork.com/journals/jamapediatrics/articleabstract/2769689.

[30] Eric J. Johnson, Steven Bellman, Gerald L. Lohse, Defaults, Framing, and Privacy: Why Opting In-Opting Out, Marketing Letters 13 (2002), Pages 5-15, https://link.springer.com/article/10.1023/A:1015044207315.

[31] Gunawan *supra* at note 27.