November 21, 2022

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex B)
Washington, DC 20580

RE: Commercial Surveillance ANPR, R111004

Common Sense Media submits these comments to the Federal Trade Commission's (Commission or FTC) Advanced Notice of Proposed Rulemaking (ANPR) on the prevalence of commercial surveillance and data security practices that harm consumers. Common Sense Media is the nation's leading independent nonprofit organization dedicated to helping kids and families thrive in an increasingly digital world. We provide unbiased information, sound advice, and innovative tools to help keep kids safe online. As a trusted resource, we empower parents, teachers, and policymakers to ensure that the power of media and technology is a positive force in children's lives. We appreciate the opportunity to provide the Commission with the following comments and provide specific responses to its questions in Appendices A and B.

I. The Commission has the authority to conduct a Section 18 rulemaking.

Under the FTC Act, the Commission may initiate a Section 18 rulemaking if it believes that the practices addressed in the rulemaking are "prevalent."[1] The statute does not define the term "prevalent." Oxford Dictionary defines "prevalent" as something that "exists or is very common at a particular time or in a particular place."

The world wide web and all the devices we use to access the internet have become an essential part of our lives, to the point where individuals spend a daily average of seven hours online across

[1] 15 U.S.C. § 57(a) (The Commission shall issue a notice of proposed rulemaking . . . only where it has reason to believe that the unfair or deceptive acts or practices which are the subject of the proposed rulemaking are prevalent.).

all devices.[2] Children start using screens at a very young age, with the youngest children before even turning a month old. Kids up to 8 years old consume roughly two and a half hours of screen media a day.[3] Teens (13 to 18 year olds) are the most active online, spending nearly 9 hours of their day online.[4] These figures do not even include the amount of time kids and teens use devices for classes or homework. As kids' and teens' spend increasingly more time online, commercial surveillance becomes an ever more prevalent part of their lives.

II. This rulemaking is long overdue.

The industry's opportunity for self-regulation is over. Besides, the tech industry has proven that it cannot be trusted to regulate itself. Furthermore, the firms seem to be more interested in placing the onus on parents to protect children's privacy.

First, we cannot trust tech firms to be transparent. If Frances Haugen had not blown the whistle on Meta last fall, we would be oblivious to the extent of the firm's wrongdoing. For example, we would still be in the dark about its internal study from March 2020, showing that Instagram makes one in three teen girls' body image issues worse.[5] Despite Meta's knowledge about the negative impact Instagram had on its users' well-being, it neither disclosed the information or took remedial action.

Second, firms have addressed privacy concerns by rolling out new parental control features,[6] which do little to resolve the systemic harm caused by their data collection and sharing practices.[7] While these can be helpful tools, this approach is insufficient and ineffective. Parental controls

---

[2] Simon Kemp, Digital 2022: Global Overview Report (Jan. 26, 2022).
[3] Common Sense Media, The Common Sense Census: Media Use by Kids Age Zero to Eight 3 (2020).
[4] Common Sense Media, The Common Sense Census: Media Use by Tweens and Teens 3 (2021).
[5] Wells, G., Horwitz, J., & Seetharaman, D., Facebook Knows Instagram is Toxic for Teen Girls, Company Documents Show, WALL ST. J. (Sept. 14, 2021).

[6] New features have typically given parents the ability to see who their children are interacting with and the amount of time they are spending on platforms.Julie Jargon, How to Use Parental Controls on YouTube, TikTok, Instagram, and Snapchat, WALL ST. J. (Apr. 16, 2022) (detailing the parental controls YouTube, TikTok, Instagram, and Snapchat offer, and how to use them).

[7] Platforms have also rolled out features young users can use, such as Instagram's "take a break" and "nudge" features. Young users under a certain age (typically 16 years old) who sign up for platforms like TikTok and Instagram are also now defaulted to private accounts. Eric Han, Strengthening Privacy and Safety for Youth on TikTok, TikTok (Jan. 13, 2021); Sarah Perez, Instagram Now Defaults New Users Under 16 to Most Restrictive Content Setting, Adds Prompts for Existing Teens, Tech Crunch (Aug. 25, 2022). To be sure, such features may be helpful in preventing some children from becoming addicted to their devices, but they do not prevent privacy harms.

unfairly place the full burden on parents to supervise their children's online experience.[8] Children can easily controvert these controls, with some parents finding that managing their kids' online workarounds "another full-time job."[9] Moreover, these features do not resolve the algorithmic amplification of harmful content or invasive data privacy practices.[10]

We are happy to address any questions you may have, and we look forward to working with you to ensure kids and teens receive the protections they need and deserve from harmful commercial surveillance and data security practices.

Respectfully submitted,

/s/ Jolina Cuaresma
Jolina Cuaresma, Senior Counsel, Privacy and Tech Policy
Common Sense Media

/s/ Irene Ly
Irene Ly, Policy Counsel
Common Sense Media

[8] Navigating long privacy policies and terms of service and privacy settings is a daunting task for parents. It is even more difficult for parents who did not grow up with online platforms and are unfamiliar with them, and parents who either do not speak fluent English or do not have a language in which they can communicate with their child on a topic like media usage and online safety.

[9] Yoree Koh, Tech-Savvy Kids Defeat Apple's and Others' Parental-Control Features, WALL ST. J. (Dec. 19, 2021). As companies develop strengthened parental controls for parents to utilize, kids will only think of more creative and clever ways to get past them. For example, to bypass screen time limits parents set, kids can change the time zone to an earlier time, which allows them to keep opening and using apps. Julie Jargon, Kids Know How to Get Around iPhone Parental Controls. Here's How to Regain Control, WALL ST. J. (Sept. 3, 2022). Kids can also change the password to their parents' Apple IDs to block access to their accounts, thwarting their parents' attempts to block them from accessing certain apps.

[10] Unless a platform takes down harmful content, parents are unlikely to be able to shield their kids from it. The best parents can do is to view the content with their kids and have a conversation with the child on why the content may cause discomfort. Parents may also report it to the platform or indicate they dislike the content, Yet, a recent Mozilla study showed that indicating you are "not interested" or "dislike" a video on YouTube does not significantly affect a user's recommendations, only preventing 11% and 12% of bad recommendations respectively. Ivan Mehta, YouTube's 'Dislike' and 'Not Interested' Options Don't Do Much for Your Recommendations, Study Sees, Tech Crunch (Sept. 20, 2022).

APPENDIX A

To What Extent Do Commercial Surveillance Practices or Lax Security Measures Harm Consumers?

8. Which areas or kinds of harm, if any, has the Commission failed to address through its enforcement actions?

The Commission must take a more active role in addressing conduct that harms innovation and competition, such as "killer acquisitions," whereby an incumbent firm buys small innovative start-ups for the purpose of stifling innovation, eliminating future competition, or both.

When Congress enacted the Hart-Scott-Rodino Act of 1976 (HSR), it amended the Clayton Antitrust Act to require parties to (i) notify the Commission and the Antitrust Division of the Department of Justice before consummating mergers, acquisitions, or joint ventures when the transactions meet certain thresholds, and (ii) wait for the statutory period before completing deals. This waiting period provides the regulators an opportunity to review proposed transactions to determine whether they comply with antitrust laws. However, the Commission's September 2021 study of non-HSR reported acquisitions (occurring between 2010 and 2019) by the top five US companies (Alphabet/Google, Amazon, Apple, Facebook, and Microsoft) described how the largest tech firms acquired start-ups or patent portfolios undetected.

Even if the regulators had been aware of these nascent transactions, antitrust law is ill-equipped to address how online markets operate. Under traditional antitrust analysis, whether a transaction is likely to lessen competition includes:

- identifying whether the deal is between competitors (i.e., horizontal) or it is between firms at different points in the supply chain (i.e., vertical);
- defining the relevant market to measure market power; and
- assessing consumer welfare by the impact on price.

However, nascent acquisitions "involve companies that offer products that are not easily classified as substitutes or complements when compared to the incumbents' current market products," which makes it difficult to identify whether to apply a horizontal or vertical analysis.[11] Defining the relevant market for online competition is much more complex because digital markets are

[11] Eileen Li, Merger Review 2.0: Infusing CFIUS'S "Critical Technologies" Approach into Antitrust Oversight of Nascent Tech Acquisitions, 122 COLUM. L. REV. 1691, 1697 (2022).

multi-sided (i.e., serve two or more different categories of consumers). And price is often irrelevant because online services are generally free for users.

Thus, certain mergers, acquisitions, or joint ventures may not "substantially [ ] lessen competition" or "tend to create a monopoly" in violation of section 7 of the Clayton Act, or represent an unreasonable restraint on trade in violation of the Sherman Act. Yet, they harm innovation and competition under Section 5 of the Federal Trade Commission Act (FTC Act). The Commission must use its authority to challenge such transactions.

9. Has the Commission adequately addressed indirect pecuniary harms, including potential physical harms, psychological harms, reputational injuries, and unwanted intrusions?

No, the Commission does not address how unlawful conduct causes indirect pecuniary harms to consumers. Even prior to the Supreme Court's 2021 ruling in *AMG Capital v. FTC*[12]—holding that Section 13(b) of the FTC Act does not grant the agency authority to seek monetary damages when seeking injunctive relief—the Commission has generally sought monetary relief only when the unlawful conduct results in tangible or concrete financial or physical harm.

This approach, however, is problematic when addressing privacy harms. The harms that stem from unfair or deceptive data practices are often intangible and difficult to quantify. For example, the improper disclosure of personal data can cause embarrassment or reputational harm. For data breaches, affected consumers have not yet been harmed by identity theft or fraud, but the risk of future harm certainly causes anxiety or emotional distress. Moreover, the Commission's approach systematically disadvantages kids and teens because their privacy harms are expected to be nonfinancial in nature.[13]

It may also disadvantage women and teen girls. In its 2021 complaint against the health app Flo, which provides menstruation tracking and cycle prediction, the Commission acknowledged that hundreds of women were "outraged," "incredibly upset," "disturbed," "appalled," and "very angry" because the company had promised that their information would be private, and yet, shared it with an outside data analytics firm.[14] Despite recognizing these nonpecuniary harms, the Commission failed to seek equitable relief. To be clear, the Commission's action against Flo

[12] *AMG Capital v. FTC*, 593 U.S. __ (2021).

[13] Children are rarely, if ever, victims of identity theft or fraud.

[14] Complaint, In the Matter of Flo Health, Inc., Federal Trade Commission 2 (June 17, 2021).

focused on the firm's misrepresentations, not for a violation of the Health Insurance Portability and Accountability Act (HIPAA),[15] which protects the disclosure of sensitive health information without a patient's consent or knowledge. Healthcare or menstrual tracking apps are generally not subject to the statute.[16] Thus, absent assurances to the contrary, Flo and similar apps may share or monetize any data they collect. Data aggregators or brokers can resell such sensitive information to commercial entities who use it to make inferences about women.[17] Some inferences such as "expectant parent" may subject women and teens to discrimination, stigma, mental anguish, or other serious harms.[18]

Importantly, the Commission's approach has become especially problematic after the Supreme Court's June 2022 decision in *Dobbs v. Jackson Women's Health Organization* to eliminate the constitutional right to an abortion.[19] Now that states can prosecute individuals who obtain an abortion under criminal antiabortion laws,[20] the personal and sensitive data, especially relating to sexual activity or reproductive health, of women and teen girls can be used against them.[21] Thus, Flo's sharing of menstrual data–even though it precedes *Dobbs*–is highly troubling because such data is subject to re-identification. And even when firms are subject to HIPAA, they are still legally obligated to disclose health information when presented with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or an administrative request from a law enforcement official.[22]

Clearly, the nonpecuniary harms that kids, teens, and women face from unfair and deceptive data practices cause real harm. Common Sense Media believes that when commercial entities are required to pay for *all* harms caused by their unlawful conduct, firms are more incentivized to protect individuals' privacy and data rather than prioritizing their profits.

---

[15] Pub. L. No. 104-191, 110 Stat. 136 (1996).

[16] HIPAA only covers health providers, insurers, and clearinghouses, or their business partners. 45 C.F.R. § 160.103. *See also* Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet, U.S. Department of Health & Human Services (June 29, 2022).

[17] Federal Trade Commission, Data Brokers: A Call For Transparency and Accountability (May 2014).

[18] Federal Trade Commission, Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data (July 11, 2022).

[19] *Dobbs v. Jackson Women's Health*, 597 U.S. __ (2022).

[20] In the months since the ruling, abortion is now illegal in 11 states. Abortion providers as well as individuals who provide help (e.g, friends or family members) to anyone obtaining an abortion can also be prosecuted.

[21] Jay Edelson, Post-Dobbs, Your Data Will Be Used Against You, Bloomberg News (Sept. 22, 2022).

[22] *See generally* Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement.

10. Which kinds of data should be subject to a potential trade regulation rule? Should it be limited to, for example, personally identifiable data, sensitive data, data about protected categories and their proxies, data that is linkable to a device, or non-aggregated data? Or should a potential rule be agnostic about kinds of data?

As a general matter, all data, including derived data, should be subject to regulation. As long as the data is collected, purchased, acquired, maintained, or used by entities that fall within the Commission's jurisdiction, such data should be regulated to protect privacy.[23]

Common Sense Media recommends that the agency employ a two-prong approach to data regulation: (1) the Commission should be agnostic to the various data categories; and (2) it should impose data minimization principles.

We believe that any rulemaking should be agnostic to the type of data for at least three reasons:

1. While the listed data types vary in nature, each data type presents any number of privacy risks to different individuals depending on the nature of the data, its use, and the context in which it was collected. For example, the lack of protection over personally identifiable data may result in financial harm, such as identity theft and fraud for individuals who use credit products. Such data may also result in harm to familial or social standing for teens who have refrained from expressing their gender identity. For another example, the lack of privacy protections for sensitive data, such as geolocation data, may present risks of bodily harm to crime victims. Other sensitive categories, such as biometric data or health information, may make it more costly, or even impossible, to obtain a health plan or life insurance, or could compromise a woman's privacy and security when accessing reproductive health services.

2. The Commission does not know the future. First, the accelerated pace of technological innovation[24] makes it all but impossible to anticipate what the new Internet of Things (IoT)[25] devices will be and the type of data they will collect. For example, Shark Tank investors declined to finance the first video doorbell, which collects video footage once its

[23] Daniel Solove, 10 Reasons Why Privacy Matters, PRIVACY + SECURITY: NEWS, DEVELOPMENTS, AND INSIGHTS BLOG (Jan. 20, 2014).

[24] RAY KURZWEIL, The Singularity is Near: When Humans Transcend Biology (2005) (explaining why technological progress occurs at an increasingly faster rate).

[25] We use the term "Internet of Things" to mean the network of internet-connected physical objects that are embedded with sensors and other similar technologies for the purpose of collecting and sharing data with other smart devices.

sensor is triggered, because they thought it had no value. Five years later, the creator sold the doorbell (now called Ring) for a reported $1 billion to Amazon, which likely recognized the value in the data.[26] Second, the vast amount of data generated from the exponential growth of IoT devices makes it difficult to predict how such data may be used in the future. In January 2021, the research firm International Data Corporation estimated that by 2025, there will be 55.7 billion connected IoT devices, which will generate nearly 80 zettabytes of data. One zettabyte equals 1000 exabytes, a billion terabytes, or a trillion gigabytes. To put this into perspective, a Cisco analyst explained that roughly 3.873B bricks were used to build the Great Wall of China and if each Gigabyte in a Zettabyte were a brick, then 258 Great Walls of China could be built. At 80 zettabytes, then, 20,640 Great Walls of China could be built (80 * 258 Great Walls).

3. Seemingly innocuous data (e.g., an individual's movie rankings) can disclose sensitive information, such as sexual orientation.[27] Even aggregated or de-identified, anonymous data presents some measure of risk of re-identification. Aggregated data—data presented at the group level rather than by individual—is subject to reconstruction attacks where the use of statistical data can re-identify individuals.[28] With enough publicly available information or large data set(s), de-identified or anonymized data may become re-identified.[29]

Due to the uncertainty of the evolution of technology and data collection, as discussed above, Common Sense Media also recommends that any rulemaking impose data minimization principles. For example, the Commission should allow a company to collect only the data necessary to perform the service that is requested. It should also consider prohibiting certain secondary uses of

[26] Matt Burgess, All the Data Amazon's Ring Cameras Collect About You (Aug. 2, 2022).

[27] MICHAEL KEARNS & AARON ROTH, The Ethical Algorithm 25-26 (2020) (describing a lawsuit against Netflix brought by a gay consumer who alleged that the ability of re-identification of what movies she watched on the streaming platform would disclose her sexual orientation and negatively impact her life). *See also infra* fn. 29.

[28] The Census Project, Census Bureau Lead Researcher Tells Court Importance of Protecting Data (Apr. 21, 2021) (reporting on the declaration by Dr. John Abowd, the US Census Bureau's Chief Scientist in *State of Alabama v. U.S. Department of Commerce*, in which he described how the agency successfully re-identified 179 million Americans, roughly 58 percent of the population). The team conducted a "reconstruction attack" – the use of publicly released statistics derived from the confidential data – it only used 6 billion of the over 150 billion statistics that the Bureau had released). *Id.*

[29] In 2006, a PhD student and his advisor could re-identify customers from Netflix's data release that contained only the customers' ratings of the movies watched on the streaming platform. They used Netflix's data release and determined the approximate dates when customers watched a movie from comparing the released data to the publicly available Internet Movie Database (IMDB), in which people use real names to post their moving ratings. With approximate dates, they could correctly re-identify individuals 99% of the time. MICHAEL KEARNS & AARON ROTH, The Ethical Algorithm 23-26 (2020).

collected data, such as prohibiting sales to data brokers unless the data has been subjected to robust differential privacy techniques.

APPENDIX B

To What Extent Do Commercial Surveillance Practices or Lax Data Security Measures Harm Children, including Teenagers?

13. The Commission here invites comment on commercial surveillance practices or lax data security measures that affect children, including teenagers. Are there practices or measures to which children or teenagers are particularly vulnerable or susceptible? For instance, are children and teenagers more likely than adults to be manipulated by practices designed to encourage the sharing of personal information?

Kids and teens are particularly vulnerable to practices involving behavioral profiling, digital advertising, and the combination of both.

I. Though advertising to children was problematic well before the turn of the century, it was arguably a manageable concern that could be addressed without additional government involvement.

It has been well established that the prefrontal cortex of the human brain — the part that controls emotional maturity, self-image, and judgment — is not fully developed until the age of twenty-five. Moreover, as a practical matter, kids and teens simply lack the life experience that forms the basis for good decision making. It comes as no surprise then that children are prone to impulsive decision making and are not yet mature enough to make informed choices. Studies show that when compared to adults, children are more at risk for making unwise purchases[30] and more readily share personal information.[31]

In 1974, the government recognized that children could not distinguish between commercial and noncommercial content and that they could not evaluate the truthfulness or accuracy of the

[30] *See* Adriana Galvan et al., Earlier Development of the Accumbens Relative to Orbitofrontal Cortex Might Underlie Risk-Taking Behavior in Adolescents, J. NEUROSCI. (June 21, 2006).

[31] Sonia Livingstone et al., Children's data and privacy online: Growing up in a digital age. An evidence review, London School of Economics and Political Science 29 (Jan. 2019). Children "may also provide personal data passively and unconsciously when using online services like social media, provoked by the platform design and configuration" and because they "display some confusion of what personal data means and a general inability to see why their data might be valuable to anyone." *Id.* at 15.

information presented.[32] With kids susceptible to manipulation, the Federal Communications Commission issued a policy statement asking networks to voluntarily limit commercial time directed at kids.[33] In 1978, the agency issued a Notice of Proposed Rulemaking pursuant to its authority under Section 18 of the FTC Act to issue a Trade Regulation Rule regarding Children's Advertising. Specifically, the agency proposed to "[b]an all televised advertising for any product which is directed to, or seen by, audiences composed of a significant proportion of children who are too young to understand the selling purpose of or otherwise comprehend or evaluate the advertising."[34] The FTC faced severe backlash, mocked as the "National Nanny."[35] Even though the FTC abandoned its efforts,[36] Congress allowed its funding to lapse before passing the Federal Trade Commission Improvements Act of 1980. The act eliminated the agency's authority to issue any advertising trade regulation rule based on unfairness and it set forth additional steps, such as issuing an Advanced Notice of Proposed Rulemaking (ANPR) that the agency must undertake to promulgate a trade regulation rule. [37] Against this controversial history,[38] it is little wonder that the Commission now seeks to obtain a deep understanding, issuing an ANPR on Commercial Surveillance that includes well over 100 specific questions.

II. Today, there is no doubt that the Commission must address the unavoidable harm to kids and teens that stem from current online advertising practices.

In 1974, roughly $400 million was spent annually on TV advertising to children.[39] Before the Internet, it was reasonable to believe that any concerns about advertising to children could be better addressed by parents or caregivers. Back then, they could limit exposure to advertising by simply turning off the television. But now, nearly 50 years later, it is no longer a simple thing to "turn off" access to commercialism targeted at children. Aside from the eye-popping increase in

---

[32] *See* Children's Television Report and Policy Statement, 50 F.C.C.2d 1, 11 (1974) ("It is a matter of common understanding that, because of their youth and inexperience, children are far more trusting of and vulnerable to commercial 'pitches' than adults."). The Commission also noted that there was "evidence that very young children cannot distinguish conceptually between programming and advertising." *Id.*

[33] *Id.* at 362.

[34] 43 FR 17967, 17969 (Apr. 24, 1978).

[35] The FTC as National Nanny, WASH. POST (Mar. 1, 1978).

[36] Michael Decourcy Hinds, F.T.C. Drops Consideration of Rule on Children's TV Ads, N.Y. TIMES (Oct. 1, 1981).

[37] Pub. L. No. 96-252, 94 Stat. 374 (1980).

[38] For a comprehensive understanding about this turbulent time (referred to as "KidVid") in the Commission's history, see CHRIS JAY HOOFNAGLE, Federal Trade Commission Privacy Law and Policy 31-78 (2016).

[39] Federal Trade Commission, Staff Report on Television Advertising to Children 14 (1978).

how much advertising is spent to reach kids and teens,[40] the ubiquity of online media and services in the lives of children (and adults) has made it near impossible to shield kids from online ads. Young children watch their favorite cartoons and shows on YouTube as often or more often than they do on television. Kids and teens are assigned homework online. And students of all ages use the internet to participate in group activities, whether it be yearbook club, debate tournaments, or other voluntary or assigned activities.

With kids and teens susceptible to commercial manipulation and their lives increasingly occurring online,[41] they have become the prime targets of "social commerce"[42] through harmful practices involving behavioral profiling, digital advertising, and the combination of both.

A. Behavioral Profiling

Tech firms track kids' and teens' online activities. As soon as they log on, they involuntarily produce continuous data about themselves. With the exponential growth of computing power, firms can collect untold millions of user data points and apply predictive data analytics to draw inferences and create a profile on each child. Then, with the use of machine learning algorithms, firms curate each child's online experience by showing content deemed by the algorithm to be interesting or relevant based on the child's profile. The goal is to keep kids and teens engaged on the platform or website longer in order for firms to collect ever more data — to draw additional inferences — to develop a more expansive profile — to further curate children's online experience and the loop continues ad infinitum. This undoubtedly shapes (and likely limits) kids' and teens' interests, which we discuss in greater detail in our response to Question 14.

B. Digital Advertising

Despite the countless studies and reports about advertising's negative effects on children,[43] marketing tools have become so powerful that it has required a change in nomenclature. What

---

[40] Melissa Dittman, Protecting Children from Advertising, American Psychological Association Monitor on Psychology (June 2004) (reporting that $12 billion was spent on advertising to kids).

[41] Common Sense Media, The Common Sense Census: Media Use by Tweens and Teens (2021). In 2015, children, ages 8 to 12, spent a daily average of nearly 5 hours using screened devices; in 2021, that figure jumped by more than 20 percent. *Id.* at 3. For teens, ages 13 to 18, the statistics are even more alarming. In 2015, they spent roughly 40 percent of waking hours in front of screens; in 2021, that figure grew to roughly 55 percent. *Id.*

[42] Rather than separate ecommerce sites, commercial activities are merged into the social media online experience. Social Commerce Is The Path To Young, Media Savvy Consumers, PYMTS (Apr. 5, 2021).

[43] *See e.g.*, American Psychological Association, Report of the APA Task Force on Advertising and Children (Feb. 2004).

concerned regulators in the past — commercial messages distributed to a broad audience and generally interrupt programming on television or radio[44] — is now referred to as "traditional advertising" to distinguish it from "digital advertising," which is far more detrimental to kids and teens.

With advancements in technology, digital advertising purposefully blurs the line between commercial and noncommercial content, making it even more difficult for children to distinguish between the two. The new and heavily integrated advertising formats are difficult even for many adult consumers to recognize and understand.[45] Two examples of digital advertising are:

1. ***Content Marketing***

Here, ads are embedded into content (or, entertainment), allowing advertising to disguise its commercial nature by creating content such as inspirational stories, helpful articles, or funny memes that attract consumers' attention.[46] One type of content marketing is an "advergame," which involves companies partnering with video game developers to design an online game that seamlessly promotes the firm's product or service.[47]

2. ***Influencer Marketing***

Ads are depicted as "word of mouth" recommendations by content creators who have developed a large social media following. These individuals are known as "influencers." They take videos of themselves during the course of their day and post them online (i.e., vlog). Influencers can be seen using (advertised) products. And because influencers are considered as peers, kids and teens believe the recommendation to be trustworthy.[48]

Kids and teens are particularly susceptible to this type of marketing because influencers are often seen as more personable and relatable than traditional celebrities. Children tend to build a special

---

[44] Uros Stanimirovic, Is Traditional Advertising a Thing of the Past?, Brid.tv (Nov. 17, 2020).

[45] Lara Spiteri Cornish, 'Mum, Can I Play on the Internet?' Parents' Understanding, Perception, and Responses to Online Advertising Designed for Children, 33 Int'l J. of Advertising 3, 437–73 (2014).

[46] Raffaello Rossi & Agnes Nairn, How Children Are Being Targeted With Hidden Ads on Social Media, The Conversation (Nov. 3, 2021).

[47] *See e.g.*, Mitch Swanson, Advergaming: How Video Game Advertising Helps With Consumer Engagement, Gamify (listing examples of popular advergames). While firms have been using advergames since the early 1990s to raise brand awareness and increase engagement with consumers, social media has made these games more effective. All About Advergames, Concordia University St. Paul.

[48] Nearly 40 percent of 12 to 15 year-olds are not aware that influencers may be paid to include a product or brand in their vlog. Ofcom, "Children and Parents: Media Use and Attitudes Report 2017," (Nov. 29, 2017).

type of relationship with their favorite influencers: they admire them, consider them to be their friends, imagine being part of their social world, and value their advice.[49] One survey found that influencers on YouTube, Instagram, and Snapchat impact kids' and teens' purchases more than celebrities and athletes.[50] Nielsen data shows that more than three-quarters of kids trust YouTubers' recommendations on what to buy over commercials.[51]

C. Behavioral Profiling & Digital Advertising

The combination of these two practices is especially noxious for kids and teens. Based on the profiles derived from innumerable data points, marketers can create any number of ads that are customized to appeal to groups of kids with similar profiles at a relatively low cost. Most children are not even aware that ads they see are specifically tailored to capture their attention.[52]

III. The harmful effects of these practices cannot be underestimated.

Unhealthy eating habits. A U.S. study found that playing food-branded advergames increased children's consumption of unhealthy snack foods, compared to playing non-food advergames and advergames featuring healthy foods.[53] A study of Australian children ages 10 to 16 found that when kids watched food-branded YouTube video content and saw their favorite food brands advertised, they consumed more unhealthy food and drinks.[54]

Smoking or vaping. In a 2019 survey, one in four teens first learned about vaping predominantly through targeted ads and sponsored content while on social media.[55] In a 2016 report, middle

---

[49] These are known as parasocial interactions or PSIs. Donald Horton and Richard Wohl, Mass Communication and Para-Social Interaction: Observations on Intimacy at a Distance, 19 Psychiatry 3, 215–29 (1956).

[50] Generation Alpha: Preparing for the Future Consumer, Wunderman Thompson 11 (2019).

[51] Getting closer: Influencers help brands build more personal consumer connections, Nielsen (May 17, 2022)

[52] Jenny Radesky et al., Digital Advertising to Children, American Academy of Pediatrics (July 2020).

[53] Jennifer L. Harris et. al, US Food Company Branded Advergames on the Internet: Children's Exposure and Effects on Snack Consumption, 6 J. of Children & Media 1 (2012). See also Impact of Unhealthy Food Marketing on Children, Obesity Evidence Hub (summarizing the research on the effect of unhealthy food marketing on children through various types of advertising including digital media content).

[54] Heather J. Baldwin et al., Like and Share: Associations Between Social Media Engagement and Dietary Choices in Children, 21 Public Health Nutrition 17 (2018).

[55] Common Sense Media, Vaping and Teens: Key Findings and Toplines (2019). More than half of teens on TikTok saw vaping-related posts. *Id.* at 1.

schoolers were 3x—and high schoolers 2x—more likely to use e-cigarettes than their peers when they routinely saw ads for the product online.[56]

Mental health concerns, poor body image, low self-esteem. Adolescence is a time when outward appearance is "everything" to a teen. Such advertising, often promoted by influencers like the Kardashians with a specific desired body type, prey on the vulnerabilities of young people, particularly young girls.[57]

IV. Our research demonstrates the ubiquitous nature of these practices.

In our 2021 State of Kids' Privacy, Common Sense Media reviewed the privacy policies and practices of the 200 most popular apps intended for kids. We learned that:

- The practice of selling children's data to third parties has increased since 2018;[58]
- Nearly two-thirds of the apps either have unclear privacy policies or policies disclosing that kids are tracked on the app and across the internet for advertising purposes;[59] and
- The policies of at least half of these apps disclose that they may send kids targeted ads based on personal information that the company has collected about them.[60]

As kids and teens use multiple apps and online platforms, which rely almost exclusively on digital advertising revenue, children are certainly exposed to harmful advertising every day.

---

[56] Lisa Rapaport, Teens Most Drawn to E Cigarettes by Online Ads, Reuters (Apr. 2016).

[57] Hannah Preston, Detox Tea Company Uses Photo of Eating Disorder Survivor Without Consent: 'I Am Fundamentally Against Things Such As Weight Loss Teas,' Newsweek (Mar. 20, 2019); Ashleigh Carter, A Detox Tea Brand Pushed by Celebs Has to Pay $1 Million for False Advertising, Now This News (Mar. 13, 2020).

[58] Common Sense Media, 2021 State of Kids' Privacy 55-56 (2021).

[59] *Id.*

[60] *Id.* To be clear, providing these disclosures are unlikely to satisfy the requirements under the Children's Online Privacy & Protection Act, which requires companies to seek parental consent before collecting any data of kids under 13.

14. What types of commercial surveillance practices involving children and teens' data are most concerning? For instance, given the reputational harms that teenagers may be characteristically less capable of anticipating than adults, to what extent should new trade regulation rules provide teenagers with an erasure mechanism in a similar way that COPPA provides for children under 13? Which measures beyond those required under COPPA would best protect children, including teenagers, from harmful commercial surveillance practices?

The use of kids' and teens' data for commercial surveillance practices is generally problematic for one simple reason: they are still developing into who they want to become. Common Sense Media finds the combined use of profiling and algorithmic recommendations distinctly troubling because it interferes with children's personal development.

As discussed in our response to Question 13, as long as individuals are online, they involuntarily provide firms with a steady stream of data points about themselves. Such data includes information about which websites were visited and how many times as well as what content was viewed and for how long. It also includes information that provides firms with insight about users' preferences, characteristics, and interests. With predictive data analytics, firms develop inferences and create user profiles for each individual. And with machine learning algorithms,[61] firms curate each user's online experience based on the algorithmic recommendations. The goal is to keep individuals engaged to keep them online longer, allowing firms to collect ever more data — to develop better profiles — to better curate their online experience — to keep them online longer. This is a continuous feedback loop.

For kids and teens, however, this continuous feedback loop is insidious. First, they should be free to grow up without having their every thought, embarrassing moment, or mistake memorialized. Firms should be prohibited from recording children's online activities and using such data to make inferences about them. Second, kids' and teens' interests and personalities are still developing, and

[61] Algorithmic recommendation systems can also perpetuate discrimination by showing certain users opportunities but not others, or exhibit biases when making decisions. Many colleges have started using more algorithmic solutions to help make admission decisions, especially since the COVID-19 pandemic. See Rashida Richardson & Marci Lerner Miller, The Higher Education Industry Embracing Predatory and Discriminatory Student Data Practices Slate (Jan. 13, 2021). However, these methods can exclude underrepresented students and create new and less obvious barriers to higher education. "For example, some colleges have started tracking prospective student engagement through social media or using econometric modeling to determine the type of incoming class they can afford to admit." *Id.* "The methods used to track student engagement are likely to favor students with the resources to visit the colleges they are applying to and have the access to private college counselors who advise them to engage with colleges' social media accounts and by email." *Id.*

they should be encouraged to check out new things. Firms should be banned from limiting children's online experiences. The Commission should ban the use of algorithmic recommendations that supposedly identify interesting content and exclude what is deemed irrelevant or contradictory to a given child's beliefs or presumed interests.[62] Dictating what kids' and teens' view essentially affects who they become.[63] Take for example a firm that profiles a group of kids as gamers and then allows advertisers to send them messages that encourage more of this behavior. If kids click on these messages, the firm collects data that reinforces their interest in gaming and they'll likely receive even more gaming messages. Clearly, limiting the diversity of information that kids and teens encounter results in filter bubbles or echo chambers.[64] Children should not be prevented from exploring and developing other interests.

Further, kids who know they are being monitored by surveillance technology are less likely to engage in critical thinking, political activity, or questioning of authority.[65] Their expression can also be chilled, because they are fearful these ads could expose aspects of their lives they want to either keep private or share on their own terms.[66] For example, ads for LGBTQ+ resources showing up on a shared device could prematurely "out" a child to their family, rather than giving them the autonomy to do so on their own accord. Moreover, the use of profiling and algorithmic recommendations can lead to destructive or illegal behavior. For example, though 21 is generally the legal drinking age, Facebook allowed advertisers to send targeted messages to kids that the social media firm had profiled as interested in alcohol.[67]

Common Sense Media believes that firms should be banned from profiling minors (which would minimize, but not negate the need for an erasure mechanism) and subjecting them to algorithmic recommendations that can quickly devolve into algorithmic amplification. When companies fail to address the algorithmic amplification of harmful content,[68] kids and teens can be led more easily down dark rabbit holes, where their mental and physical wellbeing is at even greater risk. For example:

---

[62] Privacy International, Data Is Power: Profiling and Automated Decision-Making in GDPR 9 (2017).

[63] Common Sense Media, AdTech and Kids: Behavioral Ads Need a Time Out (May 13, 2021).

[64] *Id.*

[65] D.H. Brown & N. Pecora, Online Data Privacy as a Children's Media Right: Toward Global Policy Principles. Journal of Children and Media, 8(2), 201–207 (2014).

[66] Common Sense Media, AdTech and Kids: Behavioral Ads Need a Time Out (May 13, 2021).

[67] Children 'interested in' gambling and alcohol, according to Facebook, THE GUARDIAN (Oct. 9, 2019).

[68] Although firms are aware of such content on their platforms and that such content often violates their own community guidelines, firms are reticent to remove the harmful content. Yi Liu, Pinar Yildirim, and Z. John Zhang, Implications of Revenue Models and Technology for Content Moderation Strategies (Nov. 23, 2021).

- Self-harm and suicidal ideation. In 2017, 14-year-old Molly Russell killed herself after falling into a vortex of despair on social media the last year of her life.[69] An inquest into her death concluded that she died from "an act of self-harm while suffering from depression and the negative effects of online content."[70] Of 16,300 pieces of content Molly saved, liked, or shared on Instagram in the six months before she died, 2,100 were related to suicide, self-harm, and depression.[71] The more of this content she consumed, the more the algorithm fed her similar content. She watched 138 videos that contained suicide and self-harm content, sometimes binging them in single sessions.[72] The content was so disturbing that, at a hearing in a London coroner court, a consultant child psychiatrist said he could not sleep well for weeks after viewing the content Molly had seen right before her death.[73] The coroner even considered editing footage for the court because of how distressing the content is, but decided against it because Molly herself had no such choice.[74] Molly also used Pinterest to view similar content, and the platform had sent content recommendation emails to her with titles such as "10 depression pins you might like," even after her death.[75]

- Eating disorder content. A report by children's advocacy watchdog group Fairplay showed that Meta knowingly profited from pushing eating disorder content to children on Instagram since at least 2019.[76] This pro-eating disorder bubble on Instagram includes 90,000 unique accounts that reach 20 million unique followers, and at least one-third of the followers are underage.[77] Moreover, girls have developed eating disorders after being

[69] John Naughton, Molly Russell was Trapped by the Cruel Algorithms of Pinterest and Instagram, THE GUARDIAN (Oct. 1, 2022).

[70] *Id.*

[71] *Id.*

[72] Dan Milmo, 'The Bleakest of Worlds': How Molly Russell Fell into a Vortex of Despair on Social Media, THE GUARDIAN (Sept. 30, 2022).

[73] *Id.*

[74] Molly Russell Inquest: Instagram Clips Seen by Teen "Most Distressing," BBC News (Sept. 23, 2022).

[75] *Id.* In 2019, Instagram announced it would no longer allow any content depicting graphic self-harm, such as cutting, on the platform. Shanti Das, Instagram Still Hosting Self-Harm Images After Molly Russell Inquest Verdict, THE GUARDIAN (Oct. 8, 2022). Yet, simple keyword searches on the platform last month showed that many of these images are still live. *Id.*

[76] Fairplay, Designing for Disorder: Instagram's Pro-eating Disorder Bubble (Apr. 2022).

[77] Id. The speed with which a user's feed can become overwhelmed with this kind of content is further alarming. Within a day of U.S. Senator Richard Blumenthal (D-CT)'s office creating a fake Instagram account for a 13-year-old girl and following accounts with content related to disordered eating and dieting, the platform began recommending content promoting eating disorders and self-harm. Protecting Kids Online: Snapchat, TikTok, and YouTube, Hearing Before the Subcommittee on Consumer Protection, Product Safety, and Data Security, Oct. 26, 2021 (Statement of Richard Blumenthal); *See also* Adam Westbrook, Lucy King, and Jonah M. Kessel, What's One of the Most Dangerous Toys for Kids? The Internet, N.Y. TIMES (Nov. 24, 2021).

subjected to such content. For example, after watching one video by a fitness influencer on TikTok and following her, a teen user named Lauren's feed became dominated by content focused on keeping up a so-called "healthy" lifestyle that pushed her to the dangerous trend of meticulously tracking how many calories they eat.[78] She went from feeling positively about her body, to crying about it every night after watching videos of people saying they hated their body. Four months later, she was diagnosed with an eating disorder.

There is no shortage of harmful content online. For example, the "blackout challenge," where people choke themselves until they pass out on camera, became viral on online,[79] killing seven kids.[80] Although platforms do not allow content that encourages dangerous or illegal activities, when you search for terms like "blackout challenge," you can still easily find examples of them online.

15. In what circumstances, if any, is a company's failure to provide children and teenagers with privacy protections, such as not providing privacy-protective settings by default, an unfair practice, even if the site or service is not targeted to minors? For example, should services that collect information from large numbers of children be required to provide them enhanced privacy protections regardless of whether the services are directed to them? Should services that do not target children and teenagers be required to take steps to determine the age of their users and provide additional protections for minors?

The Commission should impose privacy-protective settings by default in the following scenarios:

- **Scenario One:** when a firm collects kids' and teens' data during their use of a product designed specifically for them; and

- **Scenario Two:** when a firm utilizes or employs kids' and teens' data that was collected during their use of a product designed for a general audience.

Failure to take these measures constitute an unfair practice under the Federal Trade Commission Act (FTC Act). Under Section 5(a) of the FTC Act, "unfair or deceptive acts or practices in or

[78] Avani Dias et. al, The TikTok Spiral, ABC News Australia (Jul. 25, 2021).

[79] Fairplay, Dared by the Algorithm: Dangerous Challenges Are Just a Click Away (Sept. 29, 2022).

[80] Mitchell Clark, The TikTok 'Blackout Challenge' Has Now Allegedly Killed Seven Kids, The Verge (Jul. 7, 2022).

affecting commerce . . . are . . . declared unlawful."[81] The Commission's Policy Statement on Unfairness establishes a three-prong test. An act or practice is unfair when it (1) causes or is likely to cause substantial injury to consumers, (2) cannot be reasonably avoided by consumers, and (3) is not outweighed by countervailing benefits to consumers or to competition.[82]

Scenario One. When a firm designs an online site targeting minors and routinely collects data from its users, then the firm surely has knowledge that collected data includes kids' and teens' personal information.

(1) **The lack of privacy-protective settings by default for products targeted to minors causes or is likely to cause substantial injury.** We should not expect kids and teens to recognize which privacy setting is best for them. As we explained in detail in our response to Question 13, the part of a child's brain that controls judgment has yet to fully develop. They cannot appreciate the consequences of sharing personal information on platforms or websites.[83] They tend to think that the information they provide remains at a device level, or within an app or game, and that deleting information in an app will delete it permanently from the internet.[84]

As we explained in our response to Question 9, though kids' and teens' privacy violations are difficult to quantify, their injuries are nevertheless real. In footnote 12 of its Policy Statement, the Commission makes clear that "[a]n injury may be sufficiently substantial…if it does a small harm to a large number of people, or if it raises a significant risk of concrete harm."

(2) **Kids and teens cannot reasonably avoid privacy harms without default protections.** As a practical matter, many apps designed for children are for educational purposes. Thus, they often do not have a real choice in whether to use such apps. And from the moment they begin using a school-required app, they are involuntarily generating a continuous stream of data points that the firm automatically collects. Without default privacy protections, the harm begins before a kid or teen can make a change to the privacy settings.

---

[81] 15 U.S.C. § 45(a)(1).

[82] FTC Policy Statement on Unfairness.

[83] Jenny Radesky et al., Digital Advertising to Children, American Academy of Pediatrics (July 2020); 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).

[84] Kaiwen Sun et. al, "They See You're a Girl if You Pick a Pink Robot with a Skirt": A Qualitative Study of How Children Conceptualize Data Processing and Digital Privacy Risks. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21).

Furthermore, as we noted in our response to Question 18, children have a difficult time understanding the value of their data, and thus, it would be unreasonable to expect them to recognize the need to opt-out of data sharing for third-party marketing, targeted advertising, third-party tracking across the internet, or profiling purposes.

(3) **The substantial injury to kids and teens is not outweighed by countervailing benefits to consumers or competition.** A teen conducting a research project may find the use of profiling and algorithmic recommendations quite helpful. However, such limited benefit surely does not outweigh the harm that results when tech firms limit a teen's online experience.

Scenario Two. When a firm develops an online site or service targeting a general audience, and it does not intend to collect data from kids and teens, privacy-protective settings by default may not be necessary.

However, when a firm's collection of children's data exceeds an incidental amount and it utilizes or employs that data, then a firm should provide privacy-protective settings by default. For example, when a firm does not intend to collect data from kids and teens, but nevertheless does and it monetizes such data (e.g., selling to data brokers, soliciting marketers to place ads targeting kids), then surely the firm was on notice that its data practices involve children's personal information.

In this situation, the above unfairness analysis basically holds true. The substantial injury is the same whether a firm has knowledge or is on notice that it collects data from kids and teens. While general-audience apps are unlikely to be mandated for educational purposes, today's increasingly digital world means that children's lives are online.[85] Finally, the net harm is the same.

To be clear, Common Sense Media does not recommend that the government mandate that tech firms (regardless of whether their online product or service targets minors) determine the age of their users. Were the Commission to impose age verification or age assurance technologies, their use may require firms to collect additional data or unnecessarily burden small tech firms, without any corresponding benefits. More importantly, however, tech firms collect untold millions of data points on their users; they know who their users are.

[85] Common Sense Media, The Common Sense Census: Media Use by Tweens and Teens (2021). In 2015, children, ages 8 to 12, spent a daily average of nearly 5 hours using screened devices; in 2021, that figure jumped by more than 20 percent. *Id.* at 3. For teens, ages 13 to 18, the statistics are even more alarming. In 2015, they spent roughly 40 percent of waking hours in front of screens; in 2021, that figure grew to roughly 55 percent. *Id.*

16. Which sites or services, if any, implement child-protective measures or settings even if they do not direct their content to children and teenagers?

As a preliminary matter, Common Sense Media considers a company's measures or settings to be "child-protective" if data protections are embedded into the design of its product or service such that privacy is automatic. For example, when a firm provides users with the highest level of privacy protections by default (i.e., it does not require users to do anything), then the firm has implemented a child-protective measure. Basically, firms that utilize a "privacy by design" approach are those that often implement child-protective measures.

We believe that the Commission will find aspects of Apple Inc.'s "privacy by design" approach to its products and services instructive:[86]

- Its devices' default settings provide the highest level of data protection regardless of whether the user is an adult or child;
- The firm does not monetize their users' data (i.e., sell the data to third parties) and does not utilize such data for any third-party marketing, targeted advertising, third-party tracking across the internet, or profiling purposes; and
- To register an account on Apple devices, users must "opt-in" before the company can share any data with third parties.

At the same time, Apple recognizes that its users include kids and families. When an individual seeks to create a new account,[87] the firm provides the option for a parent or legal guardian[88] to create a child account (similar to creating a child profile).[89] The process requires that the parent review and consent to the parent privacy disclosure notice.[90] To be clear, however, a child account does not provide greater data protections since Apple already provides the highest level of privacy protections by default to all users. Instead, a child account improves the safety of children on the internet through such measures as restricting access to age appropriate content, allowing communication to known contacts only, and setting daily time limits for apps used on the company's devices.

---

[86] Our extensive research shows that the overwhelming majority of firms' online products or services do not utilize a privacy by design approach and fail to implement child-protective measures. See generally Common Sense Media, 2021 State of Kids' Privacy Report (Nov. 16, 2021).

[87] *See* Apple, How to create a new AppleID.

[88] *See* Apple, Families. Only a parent or legal guardian of a child may create a child account.

[89] *See* Apple, Create an Apple ID for your child.

[90] *See* Apple, Family Privacy Disclosure for Children.

17. Do techniques that manipulate consumers into prolonging online activity (e.g., video autoplay, infinite or endless scroll, quantified public popularity) facilitate commercial surveillance of children and teenagers? If so, how? In which circumstances, if any, are a company's use of those techniques on children and teenagers an unfair practice? For example, is it an unfair or deceptive practice when a company uses these techniques despite evidence or research linking them to clinical depression, anxiety, eating disorders, or suicidal ideation among children and teenagers?

Dark Patterns

Yes, design techniques that manipulate users into prolonging their online activity facilitate the commercial surveillance of kids and teens. Such techniques, often referred to as "dark patterns," are "user interface[s] carefully crafted to trick users into doing things they might not otherwise do."[91] Figure 1 categorizes those dark patterns that are more common.

Figure 1. Commonly Used Dark Patterns[92]

Category	Variant	Description
Nagging		Repeatedly request users to take action that preferences firm
Social Proof	Activity messages	False/misleading notice that others are purchasing
	Testimonials	False/misleading positive statements from customers
Obstruction	Roach motel	Asymmetry between signing up and canceling Make it easy for users gets into a situation, but difficult to get out (e.g., a premium subscription)
	Price comparison prevention	Frustrate users' attempts to make informed purchase decisions
	Intermediate currency	Require purchases in virtual currency to obscure cost
	Immortal accounts	Account and consumer info cannot be deleted

[91] Harry Brignull, Dark Patterns: Inside the Interfaces Designed to Trick You, THE VERGE (Aug. 29, 2013). Brignull, a cognitive scientist and UX designer, coined the term "dark patterns."

[92] Jamie Luguri & Lior Jacob Strahilevitz, Shining a Light on Dark Patterns, 13 J. OF LEGAL ANALYSIS 43, 53 (2021).

Category	Variant	Description
Sneaking	Sneak into basket	While users are in the process of making a purchase, include an extra item in the cart through an opt-out radio button or checkbox on a prior page
	Hidden costs	Obscure or disclose costs late in the transaction (e.g., inform user about processing fees at very last step in checkout process
	Hidden subscription/ forced continuity	Unanticipated/undesired automatic renewal Charge credit card after the free trial ends without notice and make it difficult to cancel membership
	Bait and switch	Customer received something other than what was originally advertised
Interface interference	Hidden information/ aesthetic manipulation	Visually obscure important information with design that purposefully distracts users' attention
	Preselection	Firm-friendly option is selected by default
	Toying with emotion	Emotionally manipulative framing
	False hierarchy/ pressured selling	Induce user to select more expensive version
	Trick questions	Make questions ambiguous or understandable only after careful and close review
	Disguised ad	Induce consumer to click on something that does not look like an ad
	Confirmsharing	Frame users' choice in a way that shames users into choosing firm's preference instead
	Cuteness	Obtain users' trust with attractive robot
Forced Action	Forced spam/ social pyramid/ address book leeching	Extract info about other users Ask a user for social media permissions under the pretense it will be used for a desirable outcome (e.g. finding friends), but instead spam user's contacts in a message claiming to be from user

Category	Variant	Description
	Privacy Zuckering	Trick users into sharing personal info (named after Facebook CEO Mark Zuckerberg)
	Gamification	Provide rewards through repeated use
	Forced registration	Make users believe registration is necessary
Scarcity	Low stock message	Inform users of limited quantities
	High demand message	Inform users others are buying remaining stock
Urgency	Countdown times	Show users' opportunity ending with blatant visual cue
	Limited time messages	Inform users that opportunity ends soon

While these techniques generally use psychology to take advantage of users' vulnerabilities or biases, and are deployed to get users to act against their own best interests, dark patterns are not per se unlawful. To be sure, some techniques are clearly problematic (e.g., bait and switch), but others may be commercial speech protected under the Constitution (e.g., urgency).[93] In Central Hudson Gas & Electric Corporation v. Public Service Commission of New York, the Supreme Court explained when commercial speech is protected by the First Amendment:

> [I]t at least must concern lawful activity and not be misleading. Next, we ask whether the asserted governmental interest is substantial. If both inquiries yield positive answers, we must determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest.[94]

However, this four-part test provides little guidance in the area of dark patterns. As Professor Lior J. Srahilevitz commented:

> Some of the dark pattern strategies, though, do fall into grayer areas. And so there's just not a lot of case law on whether regulating obstruction would run aground of commercial free speech protections under the Central Hudson line of cases. Or is nagging protected by the First Amendment as a sales strategy? We just don't have a lot of precedent there. We know that under certain circumstances, nagging isn't

[93] Repeatedly asking a consumer to take a certain action is plainly annoying, but not illegal. However, when it becomes harassment, the government's restriction on persistent nagging may survive a First Amendment challenge under intermediate scrutiny.

[94] *Cent. Hudson Gas & Elec. Corp v. Public Serv. Comm'n*, 447 U.S. 557, 566 (1980).

> protected by the First Amendment. Someone who asks out a coworker on a date once, probably protected, unless there's a power disparity there. Someone who asks out a co-worker repeatedly despite refusals clearly isn't exercising their free speech rights. They're engaged in sexual harassment, if the requests are pervasive. So we do have some guideposts that we can look to from other areas of law. But I do think the First Amendment issues surrounding the regulation of obstruction, of nagging, of confirm shaming, and of certain kinds of subtle visual interference, those are questions that the FTC should spend some time thinking about.[95]

Common Sense Media recommends that the Commission look to common law torts for guidance, specifically, the Eggshell-Plaintiff Doctrine. Here, a wrongdoer is liable for actual damages, not just those damages that were reasonably foreseeable. Thus, when a wrongdoer harms an individual with an "eggshell" skull, which results in greater damages than if the harm had occurred to an average individual, the wrongdoer does not escape the additional liability.[96] In other words, "you take the victim as you find them."

The Commission should apply this same concept when regulating dark patterns regardless of whether the product is designed for kids and teens or for a general audience. For example, if a firm uses an interface interference design (e.g. toying with emotion), whether that commercial speech is constitutionally protected depends on the audience.

	Protected by the First Amendment?	Outcome
Kids under 13	No. Presumptively not protected.	Firm liable.
Teens 13 and over	No. But it is a rebuttable presumption and a firm can provide evidence refuting the presumption.	Firm may be liable.
Adults	Yes. But it is a rebuttable presumption. This would allow the FTC to hold firms accountable for using dark patterns on elderly or otherwise impaired adults.	Firm is not liable.

We noted in our response to Question 13 that the prefrontal cortex, which controls emotional maturity is not fully developed until closer to adulthood. When a website sends 7 year olds a message about a worldwide shortage of candy, they are much more likely to experience anxiety than a 15 year old teenager or an adult. Therefore, Common Sense Media strongly recommends

[95] Federal Trade Commission, Dark Patterns Workshop Transcript (Apr. 29, 2021).

[96] See Victor George, The Eggshell Plaintiff, Plaintiff Magazine (Apr. 2016).

providing the greatest protections to kids under 13. In common law tort, they represent the egg-shell plaintiff.

Algorithmic Amplification

Other techniques, such as algorithmic amplification, lead kids and teens into dark rabbit holes in violation of Section 5 of the FTC Act, especially when the research shows that children's prolonged online activity is linked to clinical depression, anxiety, eating disorders, or suicidal ideation.[97] Please see response to Question 14.

18. To what extent should trade regulation rules distinguish between different age groups among children (e.g., 13 to 15, 16 to 17, etc.)?

Common Sense Media believes that online commercial trade regulation rules should distinguish between different age groups in limited circumstances. More importantly, however, the Commission must first establish certain baseline protections for all minors. When companies fail to provide baseline protections—Opt-in Consent, Data Minimization, Banning Targeted Advertising, and the Right to Deletion—to all kids and teens, they engage in unfair practices.

I. Opt-in Consent Should be a Baseline Protection for all Minors under 18.

In the absence of regulation, companies' default settings generally require consumers to "opt-out" of data collection and data sharing.[98] With respect to commercial data collection practices, there is a single federal law that governs this space, the Children's Online Privacy Protection Act (COPPA). It requires a firm to obtain parental consent prior to collecting personal information if (i) the firm's website or online service is directed to children (ii) or the firm has "actual knowledge" that a user is under 13 years old.[99] In other words, firms may collect the personal information of any user 13 or older with abandon. Set aside that companies should be required to obtain consent before collecting anyone's data, there is no equitable reason for failing to protect teens' personal information when they are more susceptible to oversharing personal information.[100]

---

[97] *See* Georgetown University, National Center for Education in Maternal and Child Health, The Relation of Social Media and Adolescent Mental Health: A Rapid Review (02/2022).

[98] Aside from it allowing them to collect personal information by default, opt-out provides "plausible deniability" (i.e., consumers could have opted-out) when there's a public backlash to intrusive practices. Hey Apple! 'Opt Out' is Useless. Let People Opt InIt's not so crazy to want Big Tech to ask for your data—and conversations with AI assistants—before they take it, WIRED (Aug. 2019).

[99] 15 U.S.C. § 6502.

[100] See Sonia Livingstone et al., Children's data and privacy online: Growing up in a digital age. An evidence review, London School of Economics and Political Science 29 (Jan. 2019).

A. The Commission should require firms to obtain consent from teens before collecting their data.

Experts believe that a reason for teens' tendency to share an inappropriate level of personal information is because they have "a general inability to see why their data might be valuable to anyone."[101] This should not come as a surprise. Today's teens were born at a time when social media platforms began to emerge. In 2003, Friendster and MySpace launched within months of each other. They were followed by YouTube in 2005, Facebook in 2006, Instagram in 2010, and Snapchat in 2011. Many of today's teens are unhappy about "sharenting."[102] Teens will tell you that they lost their privacy long ago.

However, teens would learn to understand the value of their privacy if every company were required to ask them for permission to collect and use their personal information. Common Sense Media recognizes the paradox in requiring companies to obtain consent from teens whose sense of judgment is not yet fully formed. However, adolescence is a time when teens are expected to become increasingly more independent.[103] For teens to determine whether to opt-in, however, firms must provide terms of services and privacy policies in a format they can understand.

B. For consent to be informed, the Commission should mandate that firms provide a notice of their terms of service and their privacy policies in short form.

In a 2018 UK Children's Commissioner report, a privacy lawyer rewrote Instagram's terms of service in child-friendly language,[104] taking what was 17 pages with roughly 5,000 words) and boiling it down to 1 page with about 800 words.[105] One 13-year-old girl who read the revised policy stated "[I]f they made it more easy (sic) then people would actually read it and think twice about the app."[106] This report also found that only people with postgraduate levels of

---

[101] *Id.* at 15.

[102] Why Kids are Confronting Their Parents about "Sharenting", N.Y. TIMES OPINION (2019).

[103] The European Union's General Data Protection Regulation (GDPR) recommends 16 as the age of consent, but member states may lower it to 13. Art. 8 GDPR. The UK has established 13 as the age of consent. Part 2, Chapter 2, No. 9 of the Data Protection Act of 2018 (implementing the GDPR). The California Consumer Privacy Act and the Connecticut Data Privacy Act (effective July 1, 2023) expand the opt-in consent requirement to minors under 16 years old, and allows teens between 13 and 16 years of age to consent instead of their parents. Cal. Civ. Code § 1798.120(c); P.A. 22-15 § 6(a)(7).

[104] Children's Commissioner, Growing Up Digital: A Report of the Growing Up Digital Taskforce (Jan. 2017).

[105] *Id.* at 10.

[106] *Id.*

education—which is only about 13.1 percent of U.S. adults[107]—could properly understand the 17-page version. This leaves the vast majority of American users at a clear disadvantage.

Anyone—but especially teens—should be able to read a notice containing privacy policies and terms of service, and quickly identify (i) what data is collected and for what purpose, (ii) whether that data is sold or shared to third parties, and (iii) under what circumstances may the data be shared with any other parties, such as affiliates and government bodies. To ensure this, firms must understand their responsibilities. For example, if the Commission defined "notice" to mean a communication that is concise, written in plain language, in 12 font (or 16 pixels), and provided in a timely manner (i.e., before using an app or navigating away from a site's landing page), then a firm would know that a teen's consent is valid only if provided pursuant to a communication that satisfied each listed element in the definition of "notice."

II. Data Minimization Should be a Baseline Protection for all Minors under 18.

A single ad tech firm has collected over 70 million data points about an individual by the time she reaches 13 years old.[108] Children should be allowed to grow up, to go from kids to tweens to teens to young adults, without having a permanent record of typical youthful indiscretions or a collection of their every thought and "like." Yet, our youth spend increasing amounts of time on sites that automatically capture their data, while at the same time they face pressure to share extremely personal and sensitive information about themselves and their peers, and to view this as common. One survey found that almost 25 percent of minors, ages 9 to 12, and about 33 percent of those aged 13 to 17, believe that sharing sexually explicit content was normal for their age group.[109]

The Commission should take data minimization principles and translate them into trade regulation rules. For example, mandating that firms collect only the data necessary to perform the service that is requested would be an important first step to protecting kids and teens.

III. Banning Targeted Advertising Should be a Baseline Protection for all Minors under 18.

---

[107] America Counts Staff, Number of People With Master's and Doctoral Degrees Doubles Since 2000, U.S. Census Bureau (Feb. 21, 2019). Only 36 percent of parents regularly read terms of service and privacy policies, which is unsurprising given how long and difficult they are to read.

[108] Common Sense Media, Behavioral Advertising Harms: Kids and Teens (Feb. 2022); Common Sense Media, List of Social Media Harms (Dec. 2021).

[109] Self-Generated Child Sexual Abuse Material: Youth Attitudes and Experiences in 2020, Thorn and Benenson Strategy Group, (Nov 2021).

Subjecting kids and teens to targeted advertising–let alone advertising in general–is unfair and deceptive because the prefrontal cortex of their brain (i.e., the part that controls emotional maturity, self-image, and judgment) is not fully developed until the age of twenty-five. Moreover, as a practical matter, they simply lack the life experience that forms the basis for good decision making.

Targeted advertising involves collecting millions of data points about children and applying predictive data analytics to draw inferences about them and create a profile for each child. Then ads are customized to appeal to groups of kids with similar profiles. Researchers have concluded that children are ill-equipped to identify targeted ads that exploit their tracked activity data from traditional advertising.[110] It utilizes coercive techniques and biased algorithmic decisionmaking systems, which limits kids' and teens' choices and autonomy as well as perpetuates discrimination. Targeted advertising is also linked to increased engagement in unhealthy behaviors, like consuming high-calorie, low-nutrient food and beverages, using tobacco products and electronic cigarettes, and drinking alcohol.[111]

IV. The "Right to Delete" Should be a Baseline Protection for all Minors under 18.

As noted above, kids and teens should be allowed to grow up without having a permanent record of typical youthful indiscretions. In the age of "sharenting," the "right to delete," colloquially referred to as an "erasure mechanism," Common Sense Media recommends that any individuals age 13 and over should have the right to delete any personal information collected or obtained about themselves while they were minors. Parents should also have the right to request the deletion of personal information of their children under 13.

[110] See Jun Zhao et al., 'I make up a silly name': Understanding Children's Perception of Privacy Risks Online. CHI Conference on Human Factors in Computing Systems Proceedings 2 (May 2019).

[111] Jenny Radesky et al., Digital Advertising to Children, American Academy of Pediatrics (July 2020).

21. Should companies limit their uses of the information that they collect to the specific services for which children and teenagers or their parents sign up? Should new rules set out clear limits on personalized advertising to children and teenagers irrespective of parental consent? If so, on what basis? What harms stem from personalized advertising to children? What, if any, are the prevalent unfair or deceptive practices that result from personalized advertising to children and teenagers?

Yes, the Commission should require companies (1) to limit their use of the information that they collect to the purposes of the specific services for which children or teenagers of their parents sign up and (2) ban personalized advertising (i.e., targeted advertising) to kids and teenagers, irrespective of parental consent.

As we propose in our response to question 18, the Commission should issue trade regulation rules that require all firms to engage in data minimization when handling minors' data, and prohibit personalized advertising to all minors. In our responses to Questions 13 and 14, we explain why these actions are necessary to limit commercial surveillance's harms to kids' and teens' physical and mental health and development.

Personalized advertising violates Section 5 of the FTC Act's prohibition on unfair practices.

(1) **It causes or is likely to cause substantial injury.** The injury itself that results from personalized advertising may be nonfinancial—frustration, aggravation, anxiety, inconvenience—but occurring hundreds or thousands of times per day.[112] It can also lead to serious harms to their overall physical and mental health and development over time. Dispersed among millions of kids and teens in the aggregate, the harm becomes substantial.

(2) **It cannot be reasonably avoided.** In our response to Question 13, kids' and teens' lives increasingly occur online, at their desktop or on their mobile devices. Our State of Kids' Privacy research report shows that over 75% of apps across the industry track user data for commercial purposes and many apps do so by default.[113]

---

[112] *See* Global Action Plan's Kids' for Sale Report 10 ("Much more research is needed, but assuming the GAP survey of teens' Instagram experience is broadly representative of users experience on other social media platforms, a third of 14 year olds could be exposed to 1,260 adverts a day--ten to twenty times as many adverts as children saw on TV alone. And that's before taking into account influencer posts and other less explicit forms of advertising on social media".

[113] Common Sense Media, State of Kids' Privacy 54-58 (2021).

(3) **The harms from personalized advertising are not significantly outweighed by countervailing benefits to consumers or competition.** Parents often have to pay for online products or services for their children to use, either by subscribing to the product or service or purchasing in-app items, so they do not reap economic benefits. All the while, their children's behavior and data collected on the app continue to be monetized for commercial purposes.

Personalized advertising also violates the statute's prohibition on deceptive practices.

(1) **It involves a representation, omission, or practice that is likely to mislead the consumer.** In their product page descriptions or privacy labels, mobile app developers state that they respect users' privacy and do not engage in targeted advertising. However, our research revealed these statements often conflict with their privacy disclosure notices and in their data collection and use practices.[114]

(2) **It must be examined from the perspective of a consumer acting reasonably under the circumstances.** Our research found that apps directed to kids do not provide transparent notice in their policies about how they protect kids and teens from the presence of personalized advertising on the product.[115] When parents are not provided transparent notice, then it is reasonable for them to think the company is not engaging in personalized advertising.

(3) **The representation, omission, or practice is a "material" one.** As discussed in our responses to questions 13 and 14, children and teens face a wide range of harms from personalized advertising. If companies were transparent about whether they engaged in personalized advertising, many parents may not consent to their child using the app, making this representation a material one.

23. How would potential rules that block or otherwise help to stem the spread of child sexual abuse material, including content-matching techniques, otherwise affect consumer privacy?

[114] *See* Li, Y., Chen, D., Li, Tianshi, Agarwal, Y., Cranor, L., & Hong, J.I. (2022, April 28). Understanding iOS privacy nutrition labels: An exploratory large-scale analysis of app store data. CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '22 Extended Abstracts). https://doi.org/10.1145/3491101.3519739.
[115] Common Sense Media, State of Kids' Privacy 54-58 (2021).

Trade regulation rules blocking or otherwise helping to stem the spread of child sexual abuse material (CSAM) may adversely affect consumers' privacy. Undoubtedly, we need to stop the dissemination of CSAM. And as our comments make clear, the lack of privacy protections cause real harm to kids and teens. Therefore, the Commission must limit privacy harms if it pursues rulemaking in this space.

Hashing[116] and text-based grooming indicators[117] are the two main technologies used to stop the spread of CSAM and child sexual exploitation. Hashing technology involves training the program to search only for specific child sexual abuse imagery[118] while text-based grooming produces an alert when a combination of specific indicators are present in a user's background and their messages. These technologies do not understand conversations or images, and thus, some level of human involvement is required (i.e., manual review of the images or the messages). As this raises privacy concerns, any data collection or use should be strictly limited to the primary purpose of stopping the spread of CSAM.

[116] A type of hashing technology is PhotoDNA, Microsoft. hash values serve as unique digital fingerprints that are assigned to pieces of data such as images and videos. When an image or video is identified as containing known CSAM, the National Center for Missing and Exploited Children (NCMEC) adds the hash value to a list that is shared with technology firms. These companies then use these hash values to scan their systems (voluntarily) for the abusive content for removal. Additionally, when NCMEC receives a report about a child sexual abuse image with a known hash value, it can quickly determine if the image has already been reported, and if the child in the image has been identified.

[117] Tech companies like Microsoft and Meta have developed techniques that search for certain phrases in conversations to detect online predators trying to lure children and extort or entice them. Courtney Gregoire, Microsoft Shares New Technique to Address Online Grooming of Children for Sexual Purposes, Microsoft (Jan. 9, 2020). This involves utilizing some background information about the user themselves, as well as scanning messages for keywords and speech patterns that frequently arise in such conversations to identify threats and incidents of suspected child sexual exploitation. For example, adult predators often first try to persuade the child to send them an image of themselves, then use it to blackmail them or ask for increasingly sexualized content from the child. Grooming indicators are essential to helping rescue a child before exploitation occurs.

[118] In other words, it does not recognize any other content scanned and it is unable to catalog the content.