January 26, 2022

Federal Trade Commission  
Office of the Secretary  
600 Pennsylvania Avenue NW  
Washington, DC 20580

Re: Comment on Petition for Rulemaking by Accountable Tech, FTC-2021-0070

INTRODUCTION

Center for Digital Democracy, Common Sense, Fairplay, Parent Coalition for Student Privacy and ParentsTogether strongly support the Petition for Rulemaking to Prohibit Surveillance Advertising filed by Accountable Tech.\(^1\) We agree that this action is necessary to stop the exploitation of children and teens.\(^2\)

Surveillance advertising, also known as behavioral or targeted advertising, has become the standard business model for a wide array of online platforms with companies utilizing this practice to micro-target all consumers, including children and teens. Surveillance advertising involves the collection of vast amounts of personal data of online users, their demographics, behaviors, preferences, characteristics, and the production of inferences. To create detailed advertising profiles from this data, users are tracked across websites and devices; they are classified, sorted, and even discriminated against via targeting and exclusion; and ultimately are left vulnerable to manipulation and exploitation.

Young people are especially susceptible to the risks posed by surveillance advertising, which is why leading public health advocates like the American Academy of Pediatrics have

---

\(^2\) Pet’n for Rulemaking at 32-33.
called for a ban on surveillance advertising to children under 18 years old. Children’s and teens’ online experiences are shaped by the affordances of surveillance marketing, which entrap them in a complex system purposefully designed to manipulate their behaviors and emotions, while leveraging their data in the process. Young people are a significant audience for the real-time ad profiling and targeting apparatus operated through programmatic platforms and technologies, which poses fundamental risks to their privacy, safety and well-being.

Surveillance advertising is harmful to young people in several ways. First, young people are already more susceptible to advertising’s negative effects and surveillance advertising allows marketers to manipulate children and teens even more effectively. Second, surveillance advertising allows advertisers to target children’s individual vulnerabilities. Third, surveillance advertising can exacerbate inequities by allowing advertisers to target (or abstain from targeting) marginalized communities. Fourth, behavioral advertising is the driving force behind a complex system of data collection and surveillance that tracks all of children’s online activity, undermining young people’s privacy and wellbeing. Finally, the Children’s Online Privacy Protection Act has failed to effectively protect children under thirteen from surveillance advertising and a more expansive prohibition is needed to protect the youngest and most vulnerable users online.

For these reasons, we urge the Commission to protect children and teens by prohibiting surveillance advertising.

---

Children and Teens Are Vulnerable to Advertising

A large body of research demonstrates that children and teens are developmentally vulnerable to advertising. It has been long recognized that it is unfair to advertise to children younger than 8 years old because they cannot identify ads or recognize the persuasive intent of commercials. That is why as recently as July 2020, the American Academy of Pediatrics called on policymakers to ban all commercial advertising to children younger than 7 years old. Even advertising professionals acknowledge that children are a vulnerable advertising target group.

Modern digital marketing, which uses an array of sophisticated techniques and often blurs the boundaries between programming and advertising, is even more difficult for children to resist. Over 75% of 8- to 11-year olds cannot distinguish ads from other digital content. And only 25% of 8-15-year-olds were able to identify the top results from a Google search as advertising, even though these results are clearly labeled with the term “ad.”

Exposure to marketing is a factor in many of the most pressing problems facing children and adolescents today, including childhood obesity, substance abuse, mental health challenges, and eating disorders as well as an increase in materialism.

---

5 Radesky et. al supra note 3.
Young People are a Highly Valuable and Key Market for Surveillance Advertisers

Since the earliest days of what was called the “Information Superhighway,” young people have been key targets for behavioral and related forms of digital advertising. As previous comments submitted to the Commission on children’s privacy issues over the last 25 years make clear, kids and teens are early adopters (aka “digital natives”); spend and also influence the spending of a significant amount of money for products, including online; engage in a range of social behaviors essential to the operations of social and mobile platforms; and are a “must-have” audience to ensure that leading platforms develop their next cohort of users for digital marketing services.

As Advertising Age discussed in 2019, reviewing what the online marketing industry calls “Generation Alpha” (children), “these kids are marketing’s newest power brokers.” Two-thirds of parents, according to a survey cited in the report, “say the habits and needs of their children influenced their last technology purchase, including TVs, smartphones and tablets.”

The recent revelations from the “Facebook Files” illustrate just how valuable young people are to online platforms. As reported last October, the loss of teens by Facebook was considered an “existential threat” because of the importance of young people to user growth. Consequently, in 2018, Facebook “earmarked almost its entire global annual marketing budget to targeting teenagers, largely through digital ads…” The document revealed that Facebook was especially concerned about reaching 13-15 year olds, which it categorized as “early high school.” Facebook’s spending for this category was said to be $390 million. Teens are key to social

---


media spending and help make up the $150 billion in “collective buying power” for the “Gen Z” cohort, according to eMarketer.15

Surveillance marketers such as Google, Meta, TikTok, Snapchat and other youth-directed platforms are especially focused on generating revenues from the more than $3 billion “influencer market” in the United States. Influencers are a key component for facilitating surveillance advertising and are deployed across a range of vertical markets especially attractive to young people, such as gaming, entertainment, fast-food, ecommerce and retail.16 Young children are an especially lucrative target for influencers, as online marketers are able to “tap into a rising crop of child influencers who have their own Instagram pages and YouTube channels with subscriber counts well into the millions.”17 This combination of influencers and online ads has a significant impact on children’s behaviors for purchasing products.18 For example, they are the prime target for the online sales of toys in the US, which is a $21 billion market. It’s not surprising that youth-directed marketers flock to places where video ads and related pitches can be delivered directly to young people. The vast majority of children in the US watch YouTube, consuming its “videos more than any other type of media,” explained a recent eMarketer analysis.19

Surveillance Advertising Enables Marketers To Exploit a Child’s Vulnerabilities via Micro-Targeting and Hyper-Personalization

18 Id.
Advertisers and the technology industries engage in continuous monitoring of children and teens, following their every move throughout the digital world—their interactions with friends and acquaintances, their engagement with a growing array of digital devices and platforms, and their emotional and behavioral relationships with brands—and amassing enormous amounts of granular data about them. Through their own Big Data operations, corporations can reach directly into young people’s lives, interacting with them through branded mobile apps, tracking their online movements and geolocation, as well as driving other behaviors and purchasing patterns.

Because marketing campaigns are cross-platform in nature, they can be directed to individuals across multiple devices, following users from smartphone to television to gaming services, and targeting them in real time. With personalization techniques, marketers can tailor their messages to individuals, using artificial intelligence and machine learning to optimize their message for outcomes desired by advertisers and tech platforms. The growing use of predictive analytics and neuroscience suggests that marketers are purposefully designing campaigns to trigger unconscious, impulsive responses in viewers.

As mentioned previously, advertising often exploits children’s vulnerabilities. But while traditional contextual advertising aims to exploit the inferred characteristics of a cohort with engaging content (e.g. younger children’s tendency to emulate older peers), surveillance advertising allows advertisers to exploit the particular vulnerabilities of an individual child. Micro-targeted ads refined with A/B testing can make it harder for children and teenagers to
resist advertising. Most children also do not realize that ads can be customized to each child. These concerns are not theoretical. In a memo prepared for advertisers, Facebook boasted that it could monitor posts and photos in real time to identify the exact moment in which teenagers feel negative emotions, like feeling “insecure,” “worthless,” and in “need [of] a confidence boost.”

Surveillance advertising takes advantage of these moments of adolescent vulnerabilities continuously. As a recent report found:

Major tech platforms offer their own personalization tools. For example, Facebook’s “dynamic creative” application enables advertisers to generate multiple versions of various elements instantaneously—including video, images, and ad copy—which can be tested in order to determine the correct combination that delivers the desired result. A key goal of this practice is “to inspire positive emotional resonance and reaction” about the product brand. Kellogg’s, Pepsi and McDonald’s have each taken advantage of Google’s “Director’s Mix,” which “allows brands to dynamically embed text, audio or images within their videos to generate unlimited variations of one video…. [B]rands can customize their videos to target specific audiences and adopt hyper-targeting strategies in their video media plans,” Google explained to advertisers. The tool facilitates “mass customization” by taking “one base video and overlay[ing] different visuals and copy, creating thousands of iterations automatically.” This is then connected to what a person may be doing or has done—such as searching for something or watching a video. By working with YouTube, says Google, marketers can use the online video platform to “create hundreds or thousands of versions to match your audience segments.” Kellogg’s used the tool to promote both Rice Krispies Treats and Pringles, reporting a positive impact on sales. Market research has shown that these new forms of “personalization” are effective at driving increased sales and brand loyalty.

Surveillance advertising also allows marketers to target harmful products to those young people who are most likely to be susceptible to those ads. In April 2021, the watchdog group

---


21 Sean Levin, Facebook told advertisers it can identify teens feeling ‘insecure’ and ‘worthless’, The Guardian (May 1, 2017).

Reset Australia conducted an experiment where they targeted teens as young as 13 by requesting Facebook approve ads based on interests in alcohol, gambling, and extreme weight loss to these groups. Facebook approved the ads – which Reset Australia did not run – and the group found that Facebook appeared to collect and use young people’s data in the same way as adults, with no discernible differences between the profiles they developed for 13-17 year old users and users over 18. These experiments were replicated by The Tech Transparency Project (TTP) in the United States.

Surveillance marketing is also used to target ads for unhealthy foods to children. Advertisers such as McDonalds target their ads to Gen Z (those born between 1997 and 2012), which includes children as young as 10. For example, McDonald’s has promoted their food in collaboration with celebrities popular with Gen Zers, such as K-Pop supergroup BTS. One such promotion featuring reggaeton singer J Balvin offered a free Oreo McFlurry to anyone who ordered from their smartphone.

**Surveillance Advertising is Inherently More Manipulative for Children and Teens than Traditional Forms of Advertising**

Surveillance advertising gives advertisers vast information about the likes, dislikes, habits, and preferences of children and teens, while children and teens do not understand how

---

24 *Id.*
28 *Id.*
surveillance advertising works and how it can affect them. Children are uniquely vulnerable to the persuasive effects of advertising because of immature critical thinking skills and impulse inhibition.29

Recent research demonstrates that children have at best a limited understanding of surveillance advertising. A study of 4–10- year-olds found that children “incorrectly perceived data tracking to be at the one-to-one interpersonal scales, data collection and tracking purposes to be for user convenience, and digital privacy risks to be primarily involving interpersonal interactions online rather than also viewing companies as privacy threats. A common missing piece is that children did not accurately conceptualize companies’ role in data processing and were not aware of automated data collection, surveillance and analysis, or the monetary incentives driving surveillance capitalism.”30

Even when children and teens recognize advertising, they are often unable to resist it when it is encouraged by celebrity influencers, embedded within trusted social networks, or delivered next to personalized content.31

A review of the literature on “datafication” of children concluded that school-aged children up to teenagers do not comprehend the full complexity of how data is collected, analyzed, and used for commercial purposes.32 Some studies suggest that teenagers have a more interpersonal and less technical conceptualization of privacy, which can make them less aware of the ramifications of sharing data with companies compared to sharing private information with

29 Radesky supra note 3.
30 Sun supra note 17.
31 Radesky supra note 3.
32 Id.
family or friends.³³ Kids and teens also do not understand the consequences of their sharing.³⁴ They tend to think that the information they share remains at a device level, or within an app or game, and that deleting the information within an app will delete it from the internet.³⁵ Young children are also more trusting of privacy-invasive technologies such as location trackers.³⁶ Teens are particularly vulnerable to online surveillance advertising because they spend so much time online.³⁷ Moreover, they tend to be much more impulsive, more emotional, more likely to take risks, feel subject to peer pressure, and not to understand the consequences of their actions.

In short, children and teens are ill-equipped to understand a complex advertising ecosystem that includes data mining, machine learning, and real-time bidding. By contrast, the advertisers, with their vast troves of data, understand practically everything about individual children, including their browsing history, mood, insecurities, their peers’ interests, and more. This power imbalance makes surveillance advertising inherently more manipulative than contextual digital advertising, let alone traditional analog advertising.

**Surveillance Marketing Can Limit Children’s Opportunities**

The ability to microtarget and profile users is particularly problematic for children, whose brains and identities are still developing. For healthy development, children should explore new things

³³ *Id.*
³⁵ *Id.*
³⁶ Radesky *supra* note 3.
and not worry about making mistakes. Behavioral advertising’s constant profiling and targeting of kids does a disservice to them by potentially labeling and limiting them from a very young age. Children may be profiled as gamers, impulsive purchasers, or anxious oversharers, and then be unfairly targeted by ads that encourage these behaviors.

Behavioral advertising’s profiling and targeting can also make child users hold themselves back. When children know surveillance technology is monitoring their activities, they appear less likely to engage in critical thinking, political activity, or questioning of authority. Targeted ads can also make children and teens refrain from exercising expression because they may expose aspects of their lives they would prefer to keep secret or share on their own terms. For example, a child may not appreciate ads for LGBTQ+ resources showing up on a shared device, inadvertently outing them in the process instead of allowing them the autonomy to do so themselves. This goes for other types of content as well, as any ads reflecting interests in sensitive topics or professional interests can affect children’s and teens’ privacy.

**Behavioral Advertising Produces Disparate Impact of Vulnerable and Marginalized Communities, Exacerbating Inequities**

The targeting or excluding of online users in surveillance advertising campaigns based on user data is inherently about making choices on how to treat users differently. It is inherently about discrimination. This automated discrimination at scale exacerbates social, economic, and political inequities as the underlying user profiles reflect and incorporate historic discrimination,

---

39 *Id.*
40 *Id*
segregation, and inequities based on racialized classifications. It is particularly egregious to allow the youngest and most vulnerable among us who are early in their lives’ journeys to be subjected to this harm via surveillance advertising, as the effects potentially replicate cumulative disadvantage across a variety of social domains, including housing, education, finance, employment, health, and political influence. As we aim to reduce historic injustice and cumulative disadvantage of marginalized communities, we must end the practice of surveillance advertising, including those of children and teens.

A growing body of academic research has documented how surveillance advertising systems lead to disparate impacts on communities of color, low-income groups, and other vulnerable members of the population. For example, studies have shown that some algorithmic decision-making may disproportionately impact members of already disadvantaged groups. “Discrimination by association” has become commonplace in the online advertising industry, where people are grouped according to their assumed interests or inferred traits and offered or excluded from different products, services, or prices on the basis of their presumed affinity. Researchers who studied Facebook’s advertising systems found that even when housing and employment ads were deliberately placed to avoid any form of discriminatory targeting based on race or gender, the platform’s ad-delivery optimization engine “skewed” the delivery of those ads

along race and gender lines anyway. Several studies have documented similar patterns beyond housing and employment.

Businesses similarly constrain children’s and teens’ choices and autonomy by using coercive techniques that only show them certain opportunities but not others, and by algorithmic profiling that builds in bias when making determinations such as when to admit students into educational programs. This selective profiling can disadvantage kids and subject them to harm based on attributes like their purported race or ethnicity, family income, or location.

One major example of this involves Naviance, a software that nearly two-thirds of American high schoolers use in the college application process. For colleges, it is a targeted advertising platform that allows admissions officials to select what kinds of students will see their recruiting messages based on factors like the students’ location, academic “ability,” the majors they’re interested in, and most problematically, even their race. The Markup found that one university deliberately advertised on Naviance only to white students, while several other schools used the platform to target students of all races in some states but only white students in other states. Naviance’s more than 10 million students can use its SuperMatch feature, which calculates a “fit score” designed to show students how well-matched they are with a specific

47 Id.
48 Id.
49 Id.
50 Id.
school.\textsuperscript{51} They can also receive messages through the software about schools that may be good matches for them, but some of those messages are advertisements paid for by the schools.\textsuperscript{52} One professor views the social engineering at play by Naviance as an electronic form of gatekeeping.\textsuperscript{53} This prevents some students from having the same access to college information on Naviance as others, which can affect their educational opportunities and what schools they see as being viable choices for them.

**Surveillance Advertising Puts Children At Risk Through Data Collection and Maximizing Engagement**

To deliver surveillance advertising, a tremendous amount of data is collected from and about children, which is harmful to them for many reasons. In 2017, research from technology company SuperAwesome estimated that by the time a child turns 13, advertisers already possess over 72 million data points about them.\textsuperscript{54} Neither children nor their parents can reasonably be expected to know what data is collected and how it is used, and to exercise meaningful control over it. Data collected for one purpose can end up being used for entirely different and even harmful purposes. Moreover, the more data that has been collected, the more sensitive information is vulnerable to a data breach and use for malicious purposes such as identity theft.\textsuperscript{55}

In order to deliver as much surveillance advertising as possible, platforms also use the massive amounts of data they collect from children to serve the personalized content most likely

\textsuperscript{51} Id.
\textsuperscript{52} Id.
\textsuperscript{53} Id.
\textsuperscript{54} Super Awesome, SuperAwesome launches Kid-Safe Filter to prevent online ads from stealing children’s personal data, (Dec. 6, 2018).
\textsuperscript{55} Javelin, Child Identity Fraud: A Web Of Deception And Loss, (Nov. 2021).
to keep children engaged. This harms children in two ways. First, the model depends on collecting massive amounts of personal data and encourages users to stay engaged online as long as possible so that more data can be collected and more ads served. For children and teens, this is particularly problematic because they lack the cognitive abilities and self-control to disengage with a platform that adults have. Consequently, children often have an even harder time exiting games, social media or other online platforms.

Personalization in order to maximize advertising revenue can also lead to children being exposed to harmful content. Algorithms drive 70% of viewing on YouTube. As a former YouTube engineer observed: “recommendations are designed to optimize watch time, there is no reason that it shows content that is actually good for kids. It might sometimes, but if it does, it is coincidence.” In recent years, many parents have documented how YouTube recommends knockoff versions of cartoons to young children which often contain violent, sexualized and disturbing content. Algorithmic recommendations can be particularly dangerous when they target children’s and teens’ greatest vulnerabilities. A Wall Street Journal investigation documented how TikTok users were served videos that encouraged eating disorders and discussed suicide. And Facebook whistleblower Frances Haugen described how Instagram’s algorithm targets users with content based on their interests, even if their interests are eating disorders or self harm: “They develop these feedback cycles where children are using Instagram to self-soothe but then are exposed to more and more content that makes them hate themselves.”

---

56 Joan Solsman, *YouTube's AI is the puppet master over most of what you watch*, CNET (Jan. 10, 2018).
Her observations were confirmed by an experiment conducted by Senator Richard Blumenthal’s office, which created an account for a fake 13 year-old girl that “liked” content about dieting. Within 24 hours, the account was served pro-eating disorder and self-harm content. According to Facebook’s own internal research, one in three adolescent girls say Instagram makes their eating disorders worse.61

**COPPA Does Not Adequately Protect Younger Children From Surveillance Ads**

It is important to note that the Children’s Online Privacy Protection Act (COPPA) Rule already prohibits behavioral advertising to children under age 13 without parental notice and consent. As the FTC explains, “Without parental consent, operators may not gather persistent identifiers for the purpose of behaviorally targeting advertising to a specific child. They also may not use persistent identifiers to amass a profile on an individual child user based on the collection of such identifiers over time and across different Web sites in order to make decisions or draw insights about that child, whether that information is used at the time of collection or later.”

The FTC has brought several cases against companies for violating this restriction. Most significantly, the FTC along with the New York Attorney General brought an action against YouTube which resulted in a $170 million settlement. In several other instances, the FTC brought successful actions against companies engaged in targeting ads to children on apps.

Nonetheless, many online services targeted to children, as well as those that are aware they are used by children, continue to engage in targeted ads to children. The FTC’s enforcement

---

60 Scott Pelley, “Whistleblower: Facebook is misleading the public on progress against hate speech, violence, misinformation,” CBS: 60 Minutes, (Oct. 4 2021), https://youtu.be/_Lx5VmAdZSI.
of the COPPA Rule has been inadequate to ensure compliance. Moreover, COPPA’s actual knowledge standard is difficult to prove, thus enabling companies to claim they did not know children were on their websites or apps, even if they do in fact know. Regardless of whether the FTC undertakes the rulemaking requested by Accountable Tech, the FTC should do more to enforce COPPA and use its APA rulemaking authority under COPPA to modify the COPPA Rule to make it even more explicit and clear that surveillance advertising of children under 13 is prohibited.

But these actions will not prevent surveillance advertising to children under 13 when they use websites and apps that are not directed to children, or when parents give consent. Nor does it prevent surveillance advertising to teens who are particularly vulnerable, albeit in different ways than younger children. Because surveillance advertising is harmful to children and teens, it is important to prohibit surveillance advertising to all as requested by Accountable Tech. Moreover, by doing so, it will be much easier for the FTC to ensure that companies are complying with the existing COPPA rule.

**Children and Teens Do Not Want Surveillance Ads and Cannot Reasonably Avoid Them**

Not only is surveillance advertising harmful, but children, teens, and their parents do not want it. Children and teens express negative attitudes about data collection and sharing, especially when this data is collected and shared covertly. They dislike it when apps monitor or collect private information about them. For example, in a survey by the Irish Data Protection

---

62 Sun supra note 17.
Commission, kids called targeted ads “annoying,” “unfair,” and “an invasion of privacy.” Parents do not want their kids to receive these ads either. Sixty percent of Australian parents reported that they are uncomfortable with companies targeting ads to children based on information they have obtained by tracking a child online. Similarly, 88 percent of American parents reported believing “the practice of tracking and targeting kids and teens with ads based on their behavioral profiles should be prohibited.”

Nonetheless, children and teens currently have no practical means of avoiding surveillance advertising. In many cases, they are not even aware of the surveillance. As one commentator notes, one reason why consumers don’t control their data despite the fact that 81% are concerned about its collection and use, is that data is intangible. As “a byproduct of our online activity, it is easy to ignore or forget about. A lot of data harvesting is invisible to the consumer—they see the results in marketing offers, free services, customized feeds, tailored ads, and beyond.”

Moreover, even if children and teens are aware of surveillance advertising, they cannot avoid it. The vast majority of platforms, websites, apps and other online services engage in data collection and surveillance advertising. For example, Meta, which owns Facebook, Instagram, and Whatsapp—three of the most popular and widely-used social media and messaging platforms globally with billions of active users—engages in surveillance advertising. So does YouTube, the most popular video platform for children, as well as TikTok, an app with a huge

---

63 Data Protection Commission. (Jan. 28, 2019). Know your rights and have your say! A consultation by the Data Protection Commission on the processing of children's personal data and the rights of children as data subjects under the General Data Protection Regulation.
64 Office of the Australian Information Commissioner, Australian Community Attitudes to Privacy Survey 2020.
following among teens and tweens. Teens that want to connect with friends, family, and others on social media or to watch or make videos to share, have no comparable alternatives.

The alternative of simply avoiding all internet use is even less feasible. The internet is a necessary part of modern life.67 This especially has been the case for children and teens, many of whom have had to rely on virtual learning to continue schooling during the pandemic. In 2020 alone, there was a 69% increase in the amount of time kids spent using a computer or laptop for education as most children attended school virtually because of the pandemic.68

Even when students are at school, they are still exposed to surveillance advertising. Many schools use ed tech products that engage in surveillance advertising. Common Sense Media’s review of the privacy policies of 200 of the most popular kids’ tech and ed tech applications and services found that about 60% displayed behavioral ads.69

Because it is not practicable for children and teens to avoid surveillance advertising themselves, it is necessary for the FTC to step in and prohibit this harmful practice.

CONCLUSION

The harm behavioral advertising inflicts on vulnerable kids and teens, coupled with how prominent and unavoidable this type of invasive advertising has become, necessitates banning the practice. We urge the Commission to move forward with a rulemaking to ban behavioral advertising in the interests of children, teens, and the general public.

---

67 The Internet has become an integral and largely unavoidable part of our lives, enabling us to communicate with loved ones, to study, to work, and to find a new job. Dr. Merten Reglitz, Internet access is a necessity not a luxury – it should be a basic right, University of Birmingham (Jun. 3, 2020). See also Colleen McClain et. al, The Internet and the pandemic, Pew Research Center (Sept. 1, 2021) (finding that over the course of the pandemic, the Internet became essential or important to 90 percent of Americans).

68 Ryan Tuchow, Kid device usage changing as a result of the pandemic, Kidscreen, (Feb. 19, 2021).