Behavioral Advertising Harms: Kids and Teens
A guide for policymakers and parents from Common Sense
By Katie Joseff, Misinformation and Disinformation Specialist

Advertising, particularly behavioral advertising, is the bedrock of Google's and Meta's (formerly known as Facebook) business models, comprising 97% and 81% of their 2021 revenues. Behavioral advertising, also known as surveillance advertising, is predicated on the belief that advertisements informed by personalized information will result in better sales. It incentivizes mass data extraction and is the impetus behind our unrivaled surveillance economy, which disproportionately harms vulnerable children and teens.

Due to consumers’ distrust, increasing concerns about data privacy, and mounting evidence that behavioral advertising is more expensive and less effective than contextual advertising, there has been a shift in the advertising landscape. Europe, with the General Data Protection Regulation (GDPR) and the recently proposed Digital Services Act (DSA), has laid the groundwork for a total ban on behavioral advertising. California and Vermont have passed laws that aim to give consumers the choice of opting out of targeting. Apple has changed its default privacy settings to block apps from tracking users across websites and other apps, and Chrome, Safari, and Firefox are phasing out or blocking third-party tracking cookies. Meta has banned the targeting of children under 18 based on interests, allowing targeting based only on age, gender, and location.

This brief explores the impact of behavioral advertising on children and the regulatory efforts that can protect children from these harms.

---

<table>
<thead>
<tr>
<th>Behavioral Advertising (aka Surveillance Ads, Targeted Ads)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What is behavioral, or surveillance, advertising?</strong></td>
</tr>
<tr>
<td>Tracking an individual consumer’s online activities with the intention of targeting them with advertising personalized to their interests.</td>
</tr>
<tr>
<td><strong>What data is tracked and analyzed?</strong></td>
</tr>
<tr>
<td>Searches, websites visited, content viewed, length of viewing, content clicked, physical location, address, user demographics, login information (email, etc.), credit card data (purchases), public record data from data brokers (court records, birth, marriage, divorce, bankruptcy, etc.), and more.</td>
</tr>
</tbody>
</table>

---


© Common Sense Media. All rights reserved. Common Sense and other associated names and logos are trademarks of Common Sense Media, a 501(c)(3) nonprofit organization (FEIN: 41-2024986).
### How is data tracked and collected?
Website cookies (tracking your activity), browser fingerprinting (identifying you by your browser, device, time zone, language, fonts installed, audio equipment, etc.; as a result, you can be tracked even when using Incognito mode), web and email beacons/spy pixels (tiny, pixel-size images that track what you click on and the emails you open, etc.), and IP address tracking, among other methods.

### How do advertisers reach consumers?
During the milliseconds in which a website loads or Google returns search results, our consumer profiles are broadcast to ad tech companies, and a "real-time bidding" ad auction takes place to determine which companies can sell to us.

### What is contextual advertising?
The placement of ads based on a website's context (e.g., a hotel ad on a travel website). Does not require mass data collection or targeting, and is experiencing a resurgence due to GDPR and doubts regarding the profitability of behavioral advertising.

## The Impact of Behavioral Advertising on Kids

How do kids feel about behavioral advertising? During a study of kids by Ireland's Data Protection Commission, one member of the 8- to 9-year-old cohort said that online ads "are so scary because they are pointed at you directly and not at everyone like a TV ad." Another said, "It feels like they're stalking you." Overall, 60% of kids age 7 to 17 did not want companies to use their data to target them with personalized ads. Corroborating these sentiments, a study from Common Sense found that 82% of teens are concerned that social media platforms share their data with advertisers. They are right to be concerned: Behavioral advertising exposes children to increased privacy violations, problematic targeting that exploits proclivities for gambling, alcohol, and unhealthy food, and general manipulation, shaping who they are and their self-expression.

### Privacy Violations

The sheer size of the digital footprints of today's children is nearly impossible to grasp, due to both the enormity of the data collected and the opacity of the data collection world. Although data collection of children under 13 is outlawed under COPPA, companies still collect and sell it, including some of the largest companies like Disney, Viacom, and YouTube.

- According to a 2017 study, ad tech companies have gathered at least 72 million data points on a child by the age of 13. This is a substantial underestimate, as they excluded trackers used by Facebook, Twitter, YouTube, and other social media platforms.
- A 2018 analysis of 959,000 apps from the U.S. and U.K. found that 93% of apps aimed at kids and families linked to third-party trackers, with over 28% of apps linked to more than 10 trackers.

---

8 Ibid.
Children interact with "connected toys" that record images, sounds, location, and, in some cases, heartbeat and other biometric data, and share the data via the internet. They also interact with Internet of Things (IoT) technologies like Amazon Alexa or Google Assistant, which record their voices and engage AI to perform voice recognition. The data on these devices is technically protected under COPPA, but some of the devices are targeted at general users, and thus face less scrutiny due to lack of "actual knowledge" that kids under 13 use their products. Amazon Echo Dot Kids Edition has faced blowback due to lack of transparency with parents about the data collected and an alleged software bug that prevented the deletion of kids' data.

- Children's opinions of IoT vary: In one study of 18 families, a 15-year-old girl reflected on her smart speaker, saying: "It's creepy to realize that it [the speaker] stores whatever we have ever asked the device to do. I don't care if my parents look into my use, but I don't want anybody else to be able to do that." 
- COPPA is often violated:
  - A 2018 study analyzed 5,855 Android apps that target kids and found that more than half appear to violate COPPA. Many of the potential COPPA violations were due to data collection behaviors of third-party software and were not necessarily due to code written by app developers.
  - In 2021, Viacom, Disney, and 10 advertising technology firms, as well as children's gaming apps like Subway Surfer (downloaded 1.5 billion times), settled class-action lawsuits concerning their placements of tracking software in popular children's gaming apps without parents' knowledge or consent.
  - Google was fined $170 million by the FTC in 2019 for illegally gathering children's data on YouTube—including identification codes used to track web browsing over time—without their parents' consent. The company allegedly made millions of dollars by using illegal data to target kids with ads.
  - Musical.ly, the predecessor of TikTok, was fined $5.7 million by the FTC in 2019 for gathering the email addresses, phone numbers, first and last names, and geolocation data of kids under 13.
  - In 2021, Life360, a family safety app used by 33 million people globally, was found to be selling kids' data to data brokers. Additionally, the company did not make adequate efforts to anonymize precise geolocation data.

### Problematic Targeting and Manipulation

- A 2018 study found that 96% of the most popular apps aimed at kids age 1 to 5 contain advertisements, including apps that are labeled as "educational." There are no restrictions on how many ads are shown, so ad viewing can take

---

up more time than playing the game itself. Kids are also manipulated by the use of popular cartoon characters and through the granting of “rewards” (e.g., virtual candy) for viewing ads.

- In 2020, it was found that advertisements appeared in 85% of YouTube videos aimed at kids age 0 to 8.\(^\text{21}\) Furthermore, 20% of the advertisements were age-inappropriate and contained violent content, sexual content, drugs/alcohol, or politics.
- A Facebook/Meta memo, leaked in 2017, bragged to advertisers that Facebook can identify when teenagers feel "insecure," "worthless," "stressed," "defeated," "overwhelmed," "stupid," "silly," "useless," and "need a confidence boost," among other traits.\(^\text{22}\) Today, they can target advertisements based on even more refined characteristics.
- In 2018, it was found that advertisers could target Facebook users based on interests in homosexuality, Islam, Hinduism, and other protected categories.\(^\text{23}\) Because Facebook claimed these to be "interests" and not users' personal traits, they felt they were not violating privacy. In 2016, they used a similar terminology loophole that allowed advertisers to target users based on "ethnic affinities," excluding people of certain races from seeing housing ads.\(^\text{24}\) They claimed that "ethnic affinity" was based on pages liked and that they did not collect racial data.
- In 2019, it was discovered that Facebook had categorized 740,000 kids under the age of 18 as being interested in gambling, and 940,000 as being interested in alcoholic beverages.\(^\text{25}\) While it is illegal for advertisers to target minors with gambling and alcohol ads, they can still integrate this knowledge in a way that harms children (e.g., advertising a game that contains gambling elements).
- Lastly, kids are generally impacted by surveillance. When they know their actions are being monitored, they are less likely to question authority or engage in critical thinking.\(^\text{26}\)

**Efficacy of Behavioral Advertising Is Questionable**

There is a false narrative that small businesses need behavioral advertising to reach consumers. Facebook, in particular, has pushed this self-serving narrative through its 2021 advertisement campaign featuring small businesses, which it arguably put forth in response to Apple's decision to default users to opt out of being tracked across apps.\(^\text{27}\) Google has also made claims that publishers will lose 50% of business due to Apple's policy,\(^\text{28}\) but this estimate has not been proven.

- The benefits for publishers are minimal. A 2019 analysis of a data set of millions of advertising transactions completed across multiple websites found that using web cookies/third-party trackers led to only a 4% increase in publishers' revenue, resulting in an average increase of $0.00008 per advertisement.\(^\text{29}\)

Quality of targeting is sometimes worse than not targeting at all. Another 2019 study of more than 90 third-party audiences provided by 19 of the leading data brokers found that targeting a consumer by gender varied in accuracy from 25.7% to 62.7%, with an overall average of 42.3%, which is less efficient than using nothing. Targeting by age and by households with or without children also varied dramatically in accuracy and had marginal benefits in comparison to no targeting. The researchers concluded: "Given the high extra costs of targeting solutions and the relative inaccuracy, we find that third-party audiences are often economically unattractive."

The opacity hurts brands and publishers. Considering programmatic marketing—the use of automated technology for buying ads, which is central to behavioral advertising—a 2020 study found that only 12% of 267 million ad impressions paid for by brands to be served on publishers' websites could be accounted for. Of those 12% of ads, one in six dollars spent was lost in the system. Furthermore, only 51% of the money spent by brands reached the publishers, and the remainder went to various third-party fees. The authors note that they looked only at premium advertisers and that the overall system likely features even more lost dollars.

A 2019 poll by Digiday found that 45% of publishing executives did not see a significant benefit from behavioral ads, and 23% said they caused a decline in revenue.

Contextual Advertising Is Arguably More Effective

A 2020 study by an ad tech company found that contextual targeting was more efficient than behavioral targeting in cost-per-click (48% lower), cost-per-viewable impression (41% lower), and the cost associated with reaching the intended demographic of the brand (36% lower).

In response to the GDPR, New York Times International stopped using behavioral advertising in 2018 and focused only on contextual and geographical targeting. Their digital advertising revenue increased. The Netherlands' public broadcaster, NPO, also stopped using behavioral advertising in 2020 and switched to contextual. They saw significant increases in ad revenue as well.

DuckDuckGo has used contextual advertising and keyword-based advertising, without storing or sharing users' information, since 2014 and has steadily grown their profits.
How Can We Protect Our Kids?

**We Need to Update and Better Enforce COPPA**

- COPPA 2.0, introduced by Senators Markey and Cassidy, would require user consent to collect data and track teens aged 13 to 15.  
  [37]
- We recommend lowering the "actual knowledge" standard—COPPA is only enforced for companies that know that kids under 13 use their products—to "constructive knowledge." In other words, the FTC would have to only prove that, had companies done their due diligence, they would have known they were collecting kids’ data.  
  [38] Companies would not be able to turn a blind eye as they can now when they have information that shows kids are on their platforms.

**Congress and/or the FTC Should Prohibit Behavioral/Surveillance Advertising**

- Federal legislation should ban behaviorally targeted ads for all kids under 18. If that is not possible, such ads should be banned for all under 13. On Jan. 18, 2022, the Banning Surveillance Advertising Act was introduced, which prohibits advertisers and facilitators from using personal data to target advertisements.  
  [39] "Broad" geo-targeting and contextual advertisements are expressly allowed. COPPA 2.0 would ban behaviorally targeted ads for children under 13, and allow businesses to serve behavioral ads to minors age 13 to 15 only if they receive minors' verifiable consent.
- Accountable Tech filed a rulemaking petition encouraging the FTC to ban behavioral advertising as an "unfair method of competition" since the space is dominated by Meta, Google, and other Big Tech platforms.  
  [40] Additionally, President Biden recently issued an executive order encouraging the FTC to "establish rules on surveillance and the accumulation of data" and "rules barring unfair methods of competition on internet marketplaces."  
  [41]

To learn more about our tech policy recommendations for kids and teens, visit [www.commonsensemedia.org/kids-action](http://www.commonsensemedia.org/kids-action)

Questions? Contact Irene Ly: ily@commonsense.org or Danny Weiss: dweiss@commonsense.org.

---

**Common Sense** is the nation’s leading nonprofit organization dedicated to improving the lives of all kids and families by providing the trustworthy information, education, and independent voice they need to thrive in the 21st century.

---


