COMMENTS OF THE TRANS ATLANTIC CONSUMER DIALOGUE

to the

Federal Trade Commission

Petition for Rulemaking by Accountable Tech

Docket No. FTC-2021-0070

January 26, 2022

The Trans Atlantic Consumer Dialogue (TACD) submits this comment in response to Accountable Tech's petition for rulemaking regarding a prohibition on surveillance advertising.[1] TACD supports Accountable Tech's argument that surveillance advertising constitutes an unfair business practice and encourages the Federal Trade Commission (FTC) to embark on the proposed rulemaking. In particular, TACD argues that surveillance advertising falls under the unfair practices portion of the FTC's mandate as it (i) is likely to cause (and has caused) substantial injury which is (ii) not reasonably avoidable by consumers and (iii) is not outweighed by countervailing benefits to consumers or competition.[2]

TACD has a long history of arguing for consumer protections against surveillance advertising[3], including in our recent recommendations issued to the European Union on passage of the Digital Services Act[4] and in hosting discussions between EU and U.S. leadership regarding surveillance advertising bans.[5]

Surveillance-based advertising (a common term for any targeted advertising whose structure is based on tracking or profiling individuals) has grown exponentially in prominence and now appears to be the dominant advertising business model.[6] This model depends on extensive data collection and individual tracking in order to tailor and target advertisements to individuals. This data collection, in turn, powers the "surveillance economy" in which personal data is continuously aggregated and sold between commercial actors, creating ever more invasive profiles on individuals.[7] The structure of the surveillance advertising industry poses the risk of substantial harm to individuals, acting against the fundamental right to privacy, increasing the risks to protection and security of personal data due to the volume of data

---

[1] Petition for Rulemaking: Accountable Tech, Federal Trade Commission (Dec. 26, 2021), https://www.regulations.gov/document/FTC-2021-0070-0001.

[2] See 15 U.S.C. Sec. 45(n) which sets forth the criteria for an act or practice being determined to be "unfair."

[3] TACD first alerted U.S. and EU governments to the dangers of behavioral advertising practices, and recommended regulatory action, as far back as 2011, http://tacd.org/wp-content/uploads/2013/09/TACD-INFOSOC-45-11-Behavioral-advertising.pdf

[4] https://tacd.org/tacd-publishes-resolution-on-regulating-digital-services/

[5] https://tacd.org/events/transatlantic-discussion-time-to-ban-surveillance-based-advertising/

[6] "Time to Ban Surveillance-Based Advertising," Forbrukerrådet Report, at 5 (June 2021), available at https://www.forbrukerradet.no/wp-content/uploads/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf.

[7] *Id.*

processed, and facilitating a rise in manipulation, discrimination, disinformation, radicalization, and fraud. Any potential commercial benefits of surveillance advertising pale compared to the sheer volume of harm.

Surveillance advertising causes substantial injury to individuals

Harms to individuals from surveillance advertising are significant and only continue to grow as the surveillance advertising structure continues to expand virtually unfettered. Harms from surveillance advertising are broad in scope, but we look at three specific harms below: (i) surveillance advertising stands directly at odds with and damages the right to privacy; (ii) surveillance advertising causes competition and antitrust concerns by allowing systems to promote their own products and services over others; and (iii) surveillance advertising allows for discrimination, exploitation, and manipulation in ads and offerings to individuals.

Privacy

In order to tailor marketing to individuals or groups, a large number of companies collect and process vast amounts of information about individual consumers. Data about us is processed every time we use an app, visit a website, shop in a store, or move around in public spaces (e.g., through Wi-Fi tracking). This information is aggregated, often by both the owner of the website/app and various third parties, and the data is then used for marketing and personalized services. However, this information can also be used (inadvertently or not) for purposes of discrimination, exclusion, and manipulation. Consumers are constantly manipulated into accepting comprehensive tracking through behavioral techniques or obfuscating design features ('dark patterns'), forced into commercial surveillance systems in order to access necessary services, and generally exposed to data collection without their knowledge and valid consent. The enormous amount of data also means that attempts to pseudonymize or anonymize the information have proven ineffective. The scope of data collection and sharing is so vast that it becomes practically impossible to know how personal data may be used.[8]

Competition and Antitrust

The troves of personal data available to major tech companies due to mass collection and aggregation through surveillance advertising contributes to the growing problem of stifling competition. Fueled by the exploitation of data, a handful of companies are consolidating their power and acting more and more as gatekeepers to consumers' activities online. Because of their dominance, these companies are able to collect vast amounts of data. The more data they have, the better they are able to profile consumers and trap them into using their services or target them with ads.[9] We have already seen examples of this problem, including in a 2017 European Commission decision which fined Google €2.42 billion for prioritizing its own products in product and service price comparison search results and demoting competitor results.[10] Key evidence reviewed for the Commission's decision included the substantial quantity of data held by Google (5.2 Terabytes solely of search results) and experiments

[8] See: https://privacyinternational.org/learn/adtech

[9] See: https://privacyinternational.org/learn/competition-and-data

[10] "Antitrust: Commission Fines Google €2.42 billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service," European Commission Press Release (June 27, 2017), available at https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784.

and surveys relating to the effect of search result visibility on consumer behavior.[11] While this is merely one example, it demonstrates the challenge to competition and antitrust concerns from companies holding these vast stores of data on individuals.

Discrimination, Exploitation, and Manipulation

The rise of surveillance-based marketing has contributed to the attempted manipulation of individuals and groups on an unprecedented scale. Companies in possession of large amounts of data can use algorithmic systems in attempts to decide when individuals are most susceptible to behave in certain ways or to react to particular images, sounds or messaging—giving rise to the risk of substantial misuse of personal data to discriminate against, exploit, or manipulate individuals. Historically, this has included directly targeting individuals struggling with low self-confidence with ads for beauty or diet products,[12] targeting individuals struggling with addiction with gambling advertisements,[13] steering vulnerable groups toward radicalization,[14] excluding women from viewing certain job postings,[15] excluding certain races from viewing housing advertisements,[16] modifying prices based on personal data and search history,[17] and incentivizing creating and spreading disinformation due to high click-rates.[18] Recent reports document how popular apps, such as menstruation apps[19], and websites such as mental health websites[20] share personal data without user's consent or even knowledge to companies which can then use such data for profiling and digital advertising. Automation makes the process even more opaque, and the optimization of messaging may have negative effects if unethical and harmful, yet effective methods are automated.

---

[11] *Id.*

[12] Sam Levin, *Facebook Told Advertisers It Can Identify Teens Feeling "Insecure" and "Worthless,"* The Guardian (May 1, 2017), https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens.

[13] Adam Satariano, *What a Gambling App Knows About You,* The New York Times (March 24, 2021), https://www.nytimes.com/2021/03/24/technology/gambling-apps-tracking.html.

[14] Ryan Mac, *Despite a Ban, Facebook Continued to Label People as Interested in Militias for Advertisers,* Buzzfeed News (April 7, 2021), https://www.buzzfeednews.com/article/ryanmac/facebook-militia-interest-category-advertisers-ban.

[15] Karen Hao, *Facebook's Ad Algorithms are Still Excluding Women From Seeing Jobs,* Technology Review (April 9, 2021), https://www.technologyreview.com/2021/04/09/1022217/facebook-ad-algorithm-sex-discrimination.

[16] Julia Angwin, Ariana Tobin & Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users by Race,* ProPublica (November 21, 2017), https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin.

[17] Arwa Mahdavi, *Cookie Monsters: Why Your Browsing History Could Mean Rip-Off Prices,* The Guardian (December 6, 2016), https://www.theguardian.com/commentisfree/2016/dec/06/cookie-monsters-why-your-browsing-history-could-mean-rip-off-prices.

[18] Arwa Mahdavi, *Targeted Ads Are One of the World's Most Destructive Trends. Here's Why,* The Guardian (November 5, 2019), https://www.theguardian.com/world/2019/nov/05/targeted-ads-fake-news-clickbait-surveillance-capitalism-data-mining-democracy; Joshua Braun, *How the AdTech Market Incentivizes Profit-Driven Disinformation,* ProMarket (July 2, 2019), https://promarket.org/2019/07/02/how-the-adtech-market-incentivizes-profit-driven-disinformation/.

[19] https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data

[20] https://www.privacyinternational.org/sites/default/files/2019-09/Your%20mental%20health%20for%20sale%20-%20Privacy%20International.pdf

These are by no means the only potential or actual harms of surveillance advertising. Children and teenagers are particularly vulnerable to the risks of exploitation, manipulation, and radicalization. Prevalent advertising fraud in this space damages advertisers and publishers. Unless surveillance advertising is meaningfully addressed, these harms will continue to compound.

Consumers are not reasonably able to avoid the injury

Consumers are unable to reasonably avoid surveillance advertising and its accompanying harms in the current AdTech ecosystem. Dominant companies in the space, including Google, Facebook, and Amazon, have cross-integrated themselves in such a way that most of the Internet becomes a funnel of information linking back to each company. Data sharing and exchanges between these companies and third parties further contribute to problem, creating a system where individuals' only option to avoid surveillance advertising is to stop using the Internet (and even then, avoiding tracking may not be possible as it extends into real-world actions). This despite evidence that individuals overwhelmingly choose to avoid surveillance advertising when given the option.[21]

In the surveillance-based advertising model, a few actors can obtain competitive advantages by collecting data from across websites and services. The increasing concentration of the digital advertising market is diminishing the value of publishers' first-party data and creating a race to the bottom. In practice, AdTech companies can collect data about consumers on one website (e.g., an online newspaper), combine it with the data they have about that user within its own services (e.g., social media), and then use the data to target ads toward those consumers on other websites that offer a lower price for ad placements.

Even though ad revenue from surveillance-based advertising has grown during the past few years, most of the revenue went to only a few platforms. Platforms such as Google and Facebook are estimated to account for about two-thirds of the digital ad market in the United States and around 80% in the UK. This means that money has moved away from publishers and potential competitors.

Dominant actors can abuse their positions in the digital advertising market by giving preference to their own services, as described above, which not only harms potential competitors but also leads to less choice and higher prices for consumers.

Although the prospect of ads that monitor your activities may have a significant 'creepy factor', many of the problematic issues related to surveillance-based advertising are 'invisible'. For example, it is impossible for consumers to know what personal data about them is held, how it is processed, transferred, or exploited, and by whom. It is impossible for the individual to know why some consumers are excluded from seeing certain ads or messages. Manipulation is most effective when consumers do not know whether or how they are being manipulated and are often unaware that they are in a vulnerable situation. In the digital environment, every consumer is potentially vulnerable. There are few measures consumers can take to limit these harmful effects, apart from giving up a large amount of useful and important digital (and some real-world) services.

Every consumer is vulnerable when faced with systems that covertly collect information about us, exploit it, and target us in a way that make us vulnerable by default and commercialize all online activities.

[21] Samuel Axon, *96% of US users opt out of app tracking in iOS 14.5, analytics find,* ArsTechnica (5/7/2021), https://arstechnica.com/gadgets/2021/05/96-of-us-users-opt-out-of-app-tracking-in-ios-14-5-analytics-find/.

The injury is not outweighed by benefits to consumers or competition

Any potential benefit of surveillance advertising would have to be significant to justify the scope and severity of the risks described above and the unavoidable nature of system. However, not only do viable alternatives exist, but claims regarding the benefits of surveillance advertising are dubious.

Alternative forms of digital advertising already exist and have proven to be effective sources of income for content providers. These alternative models are also based on targeting messages, but do not entail showing non-contextual ads that have no relevance for consumers.

For example, there are models where consumers who want interest-based advertising can self-report what type of ads they would like to see. With such a model, a consumer could indicate her interest in sports, travel, music, or more granular interests and receive ads that are relevant to these issues. This could be done at browser level and could ensure that ads are relevant to consumer interests without relying on surveillance or tracking.

Another example of alternative forms of digital marketing is 'contextual advertising'. Contextual advertising works by allowing advertisers to purchase ad space on particular types of webpages or websites based on the content on the page. This can be based on keywords so that, for example, ads for flights to England are placed next to articles about English football. In other words, contextual advertising allows advertisers to place ads for particular types of products and services in contexts where the ads will be displayed to consumers interested in that particular content.

In a sense, contextual advertising may be compared to 'traditional' advertising. Similar to how the advertiser in an offline marketing situation purchases ad space in a magazine for motor enthusiasts to reach that consumer segment, contextual advertising lets the advertiser target ads based on the content of a website or service rather than target them based on characteristics of the consumer. Thus, advertisers can reach relevant audiences without collecting or aggregating personal data. This sidesteps some of the most pressing privacy issues of the marketing, since different actors in the supply chain only need to know where the ad is shown, not necessarily who is seeing it.

This also increases the transparency and verifiability of the marketing, since the advertiser itself chooses what type of content or keywords trigger an ad being shown. This means that many visitors to a particular website or app will see the same ad.

Addressing surveillance advertising practices would also aid small businesses. In a recent poll, 75% of leaders of small and medium-sized businesses expressed that they believed tracking-based advertising undermines privacy and other human rights and 69% felt they had no option but to use Facebook and Google for advertising, despite discomfort with their influence.[22]

Conclusion

Surveillance advertising carries with it enormous harm to individuals that they cannot meaningfully avoid that is not outweighed by benefits. We urge the Federal Trade Commission to meaningfully respond to

[22] *France/Germany: Small Businesses Want EU to Get Tough on Google and Facebook's Invasive Advertising – New Research,* Amnesty International (January 17, 2022), https://www.amnesty.org/en/latest/news/2022/01/france-germany-small-businesses-want-eu-to-get-tough-on-google-and-facebooks-invasive-advertising-new-research/.

Accountable Tech's rulemaking petition and undertake efforts to protect consumers and curb the damage of surveillance advertising.