Trans Atlantic Consumer Dialogue

DOC NO: DIGI 01/22 **DATE ISSUED: 1 June 2022**

TACD Resolution on Banning Surveillance-Based Advertising

Introduction

Surveillance-based advertising (a common term for the practice that involves the collection, use, sharing, or otherwise processing of individual user data in order to algorithmically or otherwise automatically target individuals or groups of individuals as recipients of online advertising and marketing, also sometimes referred to as "surveillance advertising") is now the primary ad- and data-supported business model online. Having driven out traditional forms of context-based targeting methods for online advertising, the techniques and technologies embedded in surveillance-based advertising have had deleterious effects, undermining democratic discourse, economic and political equity, marketplace competition, privacy, public health, and basic consumer protections. The surveillance advertising driven digital ecosystem promoted and used by platforms such as Google/Alphabet and Facebook/Meta fuels misinformation, destroys local journalism and communities, drives unfettered consumption, manipulates, exploits, and discriminates against individuals, and malfunctions in many other not yet fully understood ways.

Though the Transatlantic Consumer Dialogue (TACD) remains mindful that technological advances can sometimes bring substantial benefit to consumers, injury to individuals, groups, communities, and society at large in exchange for negligible or nonexistent benefits to consumers or competition.[1] Surveillance-based advertising depends on the extensive collection of personal data and individual tracking in order to target advertisements and other messages to individuals or segments of individuals.

A digital data marketing "arms race" has resulted, in which the amassing and analysis of personal and other data is now regarded as essential to success, spurring leading global companies to make major investments in expanding their abilities to collect, identify, track, classify, sort, discriminate, and discard online personas to deliver hyper personalized targeted ads.

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

This data collection, in turn, powers the "surveillance economy" in which personal data is continuously aggregated, accessed, and shared between commercial entities and, in some cases, with governmental actors, creating ever more invasive profiles on individuals.[2] Profiles are deployed and used pervasively in all aspects of our lives, including in financial, health, housing, educational, and employment contexts. It affects how individuals consume and disseminate information and content, how they engage in the political process, how they behave and make decisions, and how their opportunities (or life chances[3]) are affected.[4]

The structure of the surveillance advertising industry acts against the fundamental right to privacy and equal opportunity and increases the risks of cybersecurity breaches and data leaks due to the volume of data processed. It increases the risk of discrimination, digital redlining, and threats to individuals' civil rights, freedom of choice, and equal opportunity. It also poses substantial risks to the health of public debates and the functioning of democratic institutions by facilitating targeted manipulation, discrimination, disinformation, radicalization, and fraud. These risks are particularly pronounced for marginalized, racialized, and other vulnerable populations, such as children. Any potential commercial benefits of surveillance advertising pale compared to the sheer volume of harm.

In 2011, TACD asked for the U.S. and the EU to reform "behavioral advertising." Over ten years later, it is apparent that surveillance advertising is at the root of many prevalent online harms and that reform is insufficient to address these harms. We need to prohibit the practice itself to clear the way for ethical ad practices that respect consumers' rights and freedoms and advance equity, fairness, and justice.

Recommendations

TACD resolves that the following action should be taken regarding surveillance-based advertising:

Surveillance-based advertising should be fully banned from use due to (i) the high risk of causing harm to individuals, groups, communities, and society at large, (ii) the inability of consumers to reasonably avoid being tracked through and for surveillance advertising, (iii) the inability of current and proposed mechanisms to address the damaging externalities that surveillance advertising produces, and (iv) the lack of benefits to individuals, groups, communities, and society at large compared to the harms.

---

[2] *Id.*

[3] *See* definition of the term "life chances," available at https://en.wikipedia.org/wiki/Life_chances.

[4] "Stop Commercial Surveillance," BEUC – The European Consumer Organisation (Mar. 22, 2022), available at https://www.youtube.com/watch?v=x7_iYSjXl2s.

Background

Surveillance advertising causes substantial injury to individuals

Harms to individuals from surveillance advertising are significant and only continue to grow as the surveillance advertising infrastructure embedded in websites, mobile applications, and operating systems expands 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 rights to privacy, individual autonomy, and freedom of choice;

(ii) surveillance advertising causes competition and antitrust concerns by allowing dominant firms to promote their own products and services over those of competitors; and

(iii) surveillance advertising allows for discrimination, exploitation, and the micro-targeted manipulation of public opinion.

Privacy

In order to target information to individuals or groups online, 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 and Bluetooth beacons). Data is processed to identify, track, classify, profile, sort, rank, and discard us according to the logic and whim of the marketer. Nobody can escape this processing as even the smallest amount of information can be used to create profiles and look-alike models. This information is combined with data previously collected, repackaged, and shared, often by both the owner of the device, site, or service and various third parties, and then used for targeting individuals, groups, or communities with tailored information and services. Intimate personal data collected through the surveillance ad system has reportedly also been sold to government agencies, including U.S. law enforcement contractors and the military, who then used it to target specific parts of society with discriminatory policies or investigations.[5] Recent reports document how popular apps, such as

[5] Joseph Cox, *How the U.S. Military Buys Location Data From Ordinary Apps,* VICE (November 16, 2020), available at https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x; Joseph Cox, *More Muslim Apps Worked with X-Mode, Which Sold Data To Military Contractors,* VICE (January 28, 2021), available at https://www.vice.com/en/article/epdkze/muslim-apps-location-data-military-xmode.

menstruation apps,[6] and websites, such as mental health websites,[7] share personal data without a 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.

Most individuals have no chance of knowing their privacy is being breached, as they 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 Certain groups, such as children and teenagers, are particularly vulnerable to manipulation, radicalization, and exploitation.[8] The enormous amount of personal data processed 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 collected and used.[9]

Competition and Antitrust

The troves of personal data available to major tech companies due to mass collection and aggregation contribute to the growing problem of stifling competition. Fueled by the exploitation of data through surveillance-based advertising, 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 which in turn cements their dominance. The more personal data these companies have, the better they are able to profile consumers, trap them into using their services, and target them with ads.[10] We have already seen examples of this problem, including in a 2021 ruling against Amazon where the Luxembourg National Commission for Data Protection fined Amazon €746 million for

[6] No Body's Business But Mine: How Menstruation Apps are Sharing Your Data, Privacy International (last updated October 7, 2020), available at https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data.

[7] "Your Mental Health for Sale," Privacy International Report (September 2019), available at https://www.privacyinternational.org/sites/default/files/2019-09/Your%20mental%20health%20for%20sale%20-%20Privacy%20International.pdf

[8] See Congressional Testimony of Frances Haugen (2021).

[9] *See* AdTech, Privacy International (last accessed May 9, 2022), available at https://privacyinternational.org/learn/adtech

[10] *See* Competition and Data, Privacy International (last accessed May 9, 2022), available at https://privacyinternational.org/learn/competition-and-data

using customer data for targeted advertising in violation of the GDPR.[11] Prior to this, Google was fined $57 million for not disclosing how data is collected and used across its systems for personalized advertising.[12] These examples demonstrate the challenge to competition and antitrust concerns from companies holding these vast stores of data on individuals.

Discrimination

Companies often profile their customers and target advertisements on the basis of race and other protected characteristics, or proxies thereof.[13] Even if unintended, certain profiling practices and the incentives that drive them disparately impact communities of color and other marginalized communities including women, the formerly incarcerated, immigrants, religious minorities, the LGBTQIA/+ communities, the elderly, people with disabilities, low-income individuals, and children and teens.[14] The use of consumer data to engage in race discrimination and other forms of redlining undermines equal opportunity and increases inequity.

Examples of this kind of profiling include discrimination in

- Fast food and alcohol advertisements
- Advertising of financial products
- Employment advertising [15]

[11] *Luxembourg DPA Fines Amazon 746 Million Euros For GDPR Violations,* Hunton Andrews Kurth (July 30, 2021), https://www.huntonprivacyblog.com/2021/07/30/luxembourg-dpa-fines-amazon-756-million-euros-for-gdpr-violations/.

[12] Adam Satariano, *Google is Fined $57 Million Under Europe's Data Privacy Law,* New York Times (January 21, 2019), https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html.

[13] *See* A Look at What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers, FTC Staff Report at 38 (October 21, 2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.

[14] Alex P. Miller and Kartik Hosanagar, *How Targeted Ads and Dynamic Pricing Can Perpetuate Bias*, Harvard Business Review (November 8, 2019), https://hbr.org/2019/11/how-targeted-ads-and-dynamic-pricing-can-perpetuate-bias.
Frederike Kaltheuner, *How online ads discriminate - Unequal harms of online advertising in Europe*, European Digital Rights (EDRi) (June 16, 2021), https://edri.org/wp-content/uploads/2021/06/EDRi_Discrimination_Online.pdf

[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; Julia Carpenter, *Google's Algorithm Shows Prestigious Job Ads to Men, But Not to Women. Here's Why That Should Worry You*, The Washington Post (July 6, 2015), https://www.washingtonpost.com/news/theintersect/wp/2015/07/06/googles-algorithm-shows-prestigious-job-ads-to-men-but-not-to-women-heres-why-thatshould-worry-you/.

- Housing advertising [16]

Exploitation and Manipulation

The rise of surveillance-based advertising has contributed to the manipulation, both attempted and successful, of individuals and groups on an unprecedented scale. The increasing informational asymmetry between corporations and individuals exacerbates these harms. Companies in possession of large amounts of data enable their advertising customers to use algorithmic systems to determine 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 exploit or manipulate individuals. Historically, this has included:

- directly targeting individuals struggling with low self-confidence with ads for beauty or diet products,[17]
- targeting individuals struggling with addiction with gambling advertisements,[18]
- steering vulnerable groups toward radicalization,[19]
- manipulating specific groups of voters with selective or false information,[20]
- modifying prices based on personal data, including race, gender, and other sensitive categories, and search history,[21] and
- incentivizing creating and spreading disinformation due to high click-rates.[22]

---

[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; Charge of Discrimination, Dept. Housing and Urban Development. v. Facebook Inc, FHEO No. 01-18-0323-8J at 6 (August 13, 2018), https://archives.hud.gov/news/2019/HUD_v_Facebook.pdf.

[17] 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.

[18] 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.

[19] 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.

[20] Vote Leave's Targeted Brexit Ads Released By Facebook, BBC (July 26. 2018), available at https://www.bbc.com/news/uk-politics-44966969.

[21] 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.

[22] 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-

These are by no means the only potential or actual harms of surveillance advertising. Prevalent advertising fraud in this space damages advertisers and publishers. Unless surveillance advertising is prohibited by regulation, these harms will continue to compound.

These injuries are unavoidable

Individuals and communities are unable to avoid surveillance advertising and its accompanying harms in the current AdTech ecosystem. Dominant companies in the surveillance advertising space, including Google, Facebook, and Amazon, have cross-integrated themselves into all levels of the digital advertising supply chain, in such a way that most of the Internet becomes a funnel of information linking back to a small handful of companies. Data sharing and exchanges between these companies and third parties further contribute to the 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). Evidence shows that individuals overwhelmingly choose to avoid surveillance advertising when given the option.[23]

In the surveillance-based advertising model, a few actors can obtain competitive advantages by collecting data from across millions of websites and services. The increasing concentration of the digital advertising market is diminishing the value of publishers' ad content, driving up the demand for more and more data for increased targeting 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 their own services (e.g., social media), and then use the data to target ads toward those consumers on thousands of third-party apps and websites that offer a lower price for ad placements. Those lower-price websites frequently include junk sites explicitly built to spread disinformation or other low-quality content and cash in on ad clicks.

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/.

23 Samuel Axon, 96% of US users opt out of app tracking in iOS 14.5, analytics find, ArsTechnica (May 7, 2021), https://arstechnica.com/gadgets/2021/05/96-of-us-users-opt-out-of-app-tracking-in-ios-14-5-analytics-find/ . "Big blow" for advertising on social media - new polling in France and Germany finds majority oppose personal information being used to target them with advertising on digital platforms, Global Witness (April 15, 2021), https://www.globalwitness.org/en/press-releases/big-blow-for-advertising-on-social-media-new-polling-in-france-and-germany-finds-majority-oppose-personal-information-being-used-to-target-them-with-advertising-on-digital-platforms/

Even though overall ad revenue from surveillance-based advertising has grown during the past few years, that growth almost entirely went to tech firms in possession of vast amounts of personal data who have implanted themselves as middlemen between advertisers and publishers. Ad 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. Up to 50% of advertising spend is lost to those middlemen, at the expense of publishers, online journalism, and potential competitors.[24]

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' to individuals. The sheer volume of adtech companies of all sizes involved in surveillance advertising creates a significant problem. For example, with sometimes dozens of ad companies' tracking code embedded in a single website or app, it is impossible for individuals to know what personal data about them is held, how it is processed or exploited, and with whom it is shared through the ubiquitous real-time bidding process. It is impossible for the individual to know why some consumers are excluded from seeing certain ads or messages. Manipulation is most effective when people 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, everyone is potentially vulnerable. There are few measures individuals can take to limit these harmful effects, apart from giving up a large amount of useful and important digital (and some real-world) services, and those measures are often reserved for, or require the assistance of, technical experts.

The surveillance advertising system does not benefit 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 the surveillance advertising system. However, not only do viable lower-risk alternatives exist, but claims regarding the benefits of surveillance advertising are dubious.

[24] *See* Seb Joseph and Ronan Shields, *The Rundown: Google, Meta and Amazon are On Track to Absorb More Than 50% of All Ad Money in 2022,* Digiday (February 4, 2022), https://digiday.com/marketing/the-rundown-google-meta-and-amazon-are-on-track-to-absorb-more-than-50-of-all-ad-money-in-2022/.

Alternative forms of digital advertising already exist and have proven to be effective sources of income for both content providers and advertisers. These alternative models are also based on targeting messages, but do not require the collection or personal data or the pervasive profiling of individuals.

Instead, 'contextual advertising' works by allowing advertisers to purchase ad space on particular types of webpages or websites based on the content of 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 in a context that is particularly valuable based on the aggregated knowledge a publisher, website, or app has about its audience. 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 an individual. The information used by context-based advertising is frequently aggregate data, rather than tied to an individual.[25] Thus, advertisers can reach relevant audiences without collecting and processing personal data. This not only sidesteps some of the most pressing privacy issues of surveillance advertising, but it also enables publishers and journalists to commercially leverage access to their audience without being outgunned by data brokers and Big Tech firms. It creates a business incentive for producing great online content and building up valuable audience instead of amassing personal data with information junk and fake news clicks.

Replacing surveillance with contextual ads also increases the transparency and verifiability of the market, since the advertiser itself chooses what type of content or keywords trigger an ad being shown. That is why banning surveillance advertising would also aid small businesses. In a recent poll, 75% of leaders of small and medium-sized businesses in Europe 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.[26]

[25] Keeping in mind that aggregate data must be pulled from a sufficiently broad number of subjects so that no individual subjects may still be identified, *see* Luk Arbuckle," Aggregated Data Provides a False Sense of Security," IAPP (April 27, 2020), https://iapp.org/news/a/aggregated-data-provides-a-false-sense-of-security/.
[26] *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/.

Conclusion

Surveillance advertising carries with it enormous harm to individuals, groups of individuals, communities, and society at large that they cannot meaningfully avoid that is not outweighed by benefits. We believe that this advertising should be fully banned.

TACD resources:

- TACD's Comments to the Federal Trade Commission Petition for Rulemaking by Accountable Tech regarding a prohibition on surveillance advertising (February 2022)
- Resolution on Regulating Digital Services (June 2021)
- Resolution on Behavioral advertising (June 2011)

Disclaimer: The recommendations in this resolution are not supported by TACD member Knowledge Ecology International.