To: Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Commercial Surveillance ANPR, R111004
Docket ID: FTC-2022-17752

Ranking Digital Rights Comment on Commercial Surveillance and Data Security

November, 21, 2022

Ranking Digital Rights Comment on Commercial Surveillance and Data Security

Ranking Digital Rights Comment on Commercial Surveillance and Data Security

Ranking Digital Rights (RDR) is a non-profit research and advocacy program at New America that works to advance freedom of expression and privacy on the internet by establishing global standards and incentives for companies to respect and protect the human rights of internet users and their communities. We carry out this mission by researching and analyzing the commitments, policies, and practices of major global digital platforms and telecommunication firms, based on international human rights standards. In addition to our research, we also advocate for laws and public policies that safeguard these fundamental rights.

RDR commends the Federal Trade Commission (the "Commission") for its thoughtful consideration of the problems associated with commercial surveillance, including surveillance advertising and data security, and welcomes the opportunity to respond to the announcement of proposed rulemaking (ANPR). The concerns raised by the FTC have important implications for privacy, freedom of expression, the right to non-discrimination, and the enjoyment of other fundamental rights. In the absence of robust private or public mechanisms for corporate accountability, the harms stemming from commercial surveillance practices are simultaneously less visible than they should be, as well as being increasingly dangerous and difficult to address. We conclude our comment with a set of recommendations for the Commission to consider in its future rulemaking proceedings.

RDR's Unique Expertise on Commercial Surveillance

As an organization that focuses on corporate accountability for human rights in the information and communication technology (ICT) sector, RDR has a unique understanding of how businesses can undermine human and civil rights as well as of the specific business practices that can prevent, mitigate, or remedy these harms. Our body of research, the Ranking Digital Rights Corporate Accountability Index (RDR Index), evaluates 26 publicly traded companies based in 15 countries with respect to 58 indicators related to corporate governance, freedom of expression and information, and privacy.[1] Among these companies are America's largest digital platform companies (e.g., Alphabet, Amazon, Apple, and Meta) and 12 telecommunications firms that include U.S.-based AT&T, Inc. The RDR Index enables civil society groups, investors, and policymakers to benchmark these firms in relation to normative standards for corporate transparency and rights-respecting policy and practice.

[1] *2020 Ranking Digital Rights Corporate Accountability Index Methodology*, Ranking Digital Rights (last accessed May 27, 2022), https://rankingdigitalrights.org/index2020/methodology.

More directly pertinent to the Commission's ANPR, we have also conducted extensive research, stakeholder consultations, and policy analysis on the surveillance advertising business model that is endemic to ICT firms. When referring to the "business model," we mean the systematic monitoring, collection, analysis, and monetization of users' personal information and observed behavior for digital advertising purposes. This is but one application of commercial surveillance, though it is among the most prevalent. Variously referred to as "surveillance advertising," "behavioral advertising," "targeted advertising," and "programmatic advertising," the practice relies on, and motivates, the systematic and pervasive surveillance of individuals' online and offline behavior.[2]

In March 2020, RDR produced its first report in a two-part series titled "*It's the Business Model*,"[3] in which we detailed the relationship between surveillance-based business models and the healthy functioning of democracy, explaining how digital platforms reliant on algorithmically-driven advertising systems contributed to civic dysfunction during the early months of the 2020 presidential election.[4] Our second report expanded this analysis to the context of the coronavirus pandemic, identifying how digital platforms' quest for user growth and engagement facilitated the spread of problematic narratives and disinformation. Notably, this advertising system and its quest for engagement also limited companies' willingness and ability to fully address their effects.[5] We continue to produce work analyzing these business models, including, most recently, a companion essay to our 2022 Big Tech Scorecard that outlines policy recommendations for governing online advertising.[6]

I. Commercial Surveillance: Background and Applications

(Responds to ANPR Q. 1; Q. 3; Q. 4; Q. 11)

Broadly, commercial surveillance refers to a range of business practices involving the collection of personal and behavioral information about customers and other individuals that is put toward various commercial ends, including, but not limited to, product development, market and user research, price-setting, and, of course, advertising. As the Commission rightly notes, "While, in

[2] Dipayan Ghosh, "What is Microtargeting and What is it Doing in our Politics?" *Mozilla* (Oct. 4, 2018), https://blog.mozilla.org/en/products/firefox/microtargeting-dipayan-ghosh/.
[3] "It's the Business Model: How Big Tech's Profit Machine is Distorting the Public Sphere and Threatening Democracy," *Ranking Digital Rights* (last accessed Jan. 26, 2022), https://rankingdigitalrights.org/its-the-business-model/.
[4] Nathalie Maréchal and Ellery Roberts Biddle, "It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge," *New America* (Mar. 17, 2020), https://www.newamerica.org/oti/reports/its-not-just-content-its-business-model/.
[5] Nathalie Maréchal, Rebecca MacKinnon, and Jessica Dheere, "Getting to the Source of Infodemics: It's the Business Model," *New America* (May 27, 2020), https://www.newamerica.org/oti/reports/getting-to-the-source-of-infodemics-its-the-business-model/.
[6] Nathalie Maréchal, "We Can't Govern the Internet without Governing Online Advertising. Here's How to Do it," *Ranking Digital Rights* (last accessed July 25, 2022), https://rankingdigitalrights.org/mini-report/we-must-govern-online-ads/.

theory, these personalization practices have the potential to benefit consumers, reports note that they have facilitated consumer harms that can be difficult if not impossible for any one person to avoid."[7]

A. A Brief History of Commercial Surveillance

As a general matter, the practice of digital surveillance is not new; more than 30 years ago, scholars identified the societal risks associated with ICT-enabled "dataveillance."[8] Surveillance advertising emerged at Google at the turn of the twenty-first century, when executives at what was then a fledgling search engine realized that the first-party data it held about its users' web searches could be used for advertising. Over time, the company's expanded product offerings resulted in increased user data, more companies (including, notably, what was then Facebook) adopted similar business models, and the growth of the data broker industry (companies that buy and sell data) facilitated the trade and use of third-party data. What started as a way for otherwise unprofitable companies to monetize data they already had has evolved into a now insatiable data-hungry profit machine for these same companies, now some of the most profitable on earth, as well as many others.

Our comment focuses primarily on one specific manifestation of commercial surveillance: surveillance advertising, also known as targeted, behavioral or programmatic advertising. We focus on surveillance advertising for two reasons. First, because of our own expertise on the subject matter, and second, because of its seminal role in the rise of surveillance capitalism—an economic system centered around the capture and commodification of personal data for the core purpose of profit-making.[9] In the decades since its inception at Google, surveillance capitalism has evolved to include myriad applications beyond advertising, all in service of drawing ever-finer distinctions between people in order to engineer specific outcomes that often benefit corporate interests to the detriment of fundamental human rights. These include the use of algorithmic tools to determine benefits eligibility, triage patients competing for scarce healthcare resources, approve or deny mortgage applications,[10] and more.

B. Surveillance Advertising Is Everywhere

A fundamental challenge for the oversight of the surveillance advertising economy is its ubiquity and thus also its reliance on automation. Today, virtually all aspects of the digital environment

---

[7] Federal Trade Commission, 16 CFR PArt 464, Trade Regulation Rule on Commercial Surveillance and Data Security, at 3, https://www.ftc.gov/system/files/ftc_gov/pdf/commercial_surveillance_and_data_security_anpr.pdf.
[8] Roger Clarke, "Information Technology and Dataveillance" (1988), *Communications of the ACM*, https://dl.acm.org/doi/pdf/10.1145/42411.42413; Roger Clarke, "Dataveillance - 15 Years On, Presentation Prepared for the Privacy Issues Forum" (March 23, 2003), http://privacy.org.nz/assets/Files/97743377.pdf
[9] Shoshana Zuboff, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power" (2019). *PublicAffairs*.
[10] Emmanuel Martinez and Lauren Kirchner, "The Secret Bias Hidden in Mortgage-Approval Algorithms," *The Markup* (Aug. 25, 2021), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.

are configured to support pervasive and invasive user surveillance for the purposes of online advertising. Digital platforms that offer social networking and search functions such as Facebook, Instagram, Google, YouTube, TikTok, and Twitter each derive the majority of their income from digital advertising.[11] For instance, approximately 98% of Meta's $117 billion in revenue came from advertising in 2021.[12] Alphabet, parent company of Google and YouTube, earned $147 billion in 2020, more than 80% of which came from its digital ads business.[13] Alphabet and Meta are especially dominant in the digital advertising market, accounting for more than 50% of all digital ad spending each year for the past several years.[14] The advertising practices of these companies have been the source of significant public scrutiny, government investigations, and regulatory fines across the globe in recent years.[15]

Telecommunication firms and internet service providers (ISPs) also derive revenue from surveillance advertising.[16] ISPs are generally not known for their privacy-preserving business practices. One reason for this stems from the repeal of the 2016 Federal Communications Commission privacy regulations, a set of rules that had required ISPs to provide greater transparency about the collection of personal information and take steps to protect customers' data.[17] Based on the FTC's own research, we know that several major ISPs have engaged in advertising-related practices involving the pervasive monitoring of subscribers' online activity, serving users advertisements based on sensitive personal characteristics, and selling user data to third parties.[18]

---

[11] Greg McFarlane, "How Facebook (Meta), Twitter, Social Media Make Money From You," *Investopedia* (November 4, 2021), https://www.investopedia.com/stock-analysis/032114/how-facebook-twitter-social-media-make-money-you-twtr-lnkd-fb-goog.aspx;

[12] S. Dixon, "Meta: Advertising Revenue Worldwide 2009-2021," *Statista* (July 27, 2022), https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/.

[13] Megan Graham and Jennifer Elias, "How Google's $150 Billion Advertising Business Works," *CNBC* (May 18, 2021), https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html

[14] Max Willens, "Meta and Google's Hold on Digital Advertising Loosens as TikTok and Others Gain Share," *Insider Intelligence* (June 27, 2022), https://www.insiderintelligence.com/content/meta-google-s-hold-on-digital-advertising-loosens-tiktok-others-gain-share.

[15] Alex Hern and Jasper Jolly, "Google Fined €1.49bn bu EU for advertising violations," *The Guardian* (March 20, 2019), https://www.theguardian.com/technology/2019/mar/20/google-fined-149bn-by-eu-for-advertising-violations; Tiffany Hsu and Eleanor Lutz, "More than 1,000 Companies Boycotted Facebook. Did it Work?," *The New York Times* (August 1, 2020), https://www.nytimes.com/2020/08/01/business/media/facebook-boycott.html; Daisuke Wakabayashi and Sapna Maheshwari, "Advertisers Boycott YouTube After Pedophiles Swarm Comments on Videos of Children," *The New York Times* (February 20, 2019), https://www.nytimes.com/2019/02/20/technology/youtube-pedophiles.html

[16] Federal Trade Commission, "A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers" (Oct. 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.

[17] Alex Kang, "FCC Privacy Rule Repealed," *The Regulatory Review* (April 6, 2017), https://www.theregreview.org/2017/04/06/kang-fcc-privacy-rule-repealed/

[18] Federal Trade Commission, "A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers" (Oct. 21, 2021),

While social media and internet companies are most commonly associated with surveillance advertising, a range of other businesses also engage in the practice. Included in this group are online marketplaces such as eBay and, in particular, Amazon.[19] Not only is Amazon one of the most profitable companies in the world, it controls nearly 40% of the e-commerce market in the United States,[20] boasts a popular subscription service with 200 million users,[21] and has a suite of business offerings spanning numerous sectors of the economy. Its ads business, valued at $8.76 billion in 2022,[22] is an important and growing part of its operations. The company's success thus also depends, to a meaningful extent, on its ability to surveil and acquire third-party information about its users. This information is used directly for advertising purposes,[23] as well as for other uses meant to benefit Amazon's various business verticals.[24]

The company's recent expansion into new markets raises additional commercial surveillance concerns. The purchase of grocery chain Whole Foods, the development of physical retail stores, and Amazon's entry into the health-care market[25] all increase the scope of the company's commercial monitoring and create new opportunities for surveillance advertising while raising significant privacy and data security concerns.[26] As the non-profit, nonpartisan watchdog Campaign for Accountability has documented as part of its Tech Transparency Project, the methods by which the company tracks its users' behavior provide "extremely precise insights into the commercial, domestic, travel, social, physical, financial, and even emotional lives of its users—and their friends and family. Amazon then sells that information to advertisers in the

---

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.

[19] Stephanie Condon, "eBay sees $1 billion revenue in ad sales for FY2021, new focus on sneakers," *ZDNet* (February 23, 2022), https://www.zdnet.com/article/ebays-q4-highlights-ad-sales-luxury-goods-and-sneakers/; For a more detailed disclosure of eBay's ad practices and offerings see its dedicated "eBay Ads" website: https://www.ebayads.com/stories/reaching-in-market-shoppers-and-unique-audiences-with-an-ebay-partnership/

[20] Priya Anand, "What's Amazon's Share of Retail? Depends Who You Ask," *The Information* (June 13, 2019), https://www.theinformation.com/articles/whats-amazons-share-of-retail-depends-who-you-ask.

[21] Daniel Howley, "Amazon Prime now has 200 million members, jumping 50 million in one year," *Yahoo News* (April 15, 2021), https://news.yahoo.com/amazon-prime-has-200-million-members-142910961.html.

[22] Peter Adams, "Amazon ads top engagement ranking, but Tiktok holds innovation crown," *Marketing Dive* (September 7, 2022), https://www.marketingdive.com/news/amazon-TikTok-ad-innovation-media-spend/631295/.

[23] Megan Graham, "Amazon is Turning Advertising into its Next Huge Business - Here's How," *CNBC* (July 17, 2019), https://www.cnbc.com/2019/07/17/how-amazon-advertising-works.html.

[24] When not used for advertising, Amazon has not hesitated to make use of its 1st-party data in other problematic ways. Consider allegations that Amazon leveraged the data collected from consumers and other sellers on the platform to muscle would-be competitors out of its marketplace. See e.g., Dana Mattiolo, "Amazon Scooped Up Data from its Own Sellers to Launch Competing Products," *The Wall Street Journal* (April 23, 2020), https://www.wsj.com/articles/amazon-scooped-up-data-from-its-own-sellers-to-launch-competing-products-11587650015.

[25] Shauneed Miranda, "Amazon Buying One Medical is Only its Most Recent Dive into the Health Care Industry," *National Public Radio* (July 26, 2022), https://www.npr.org/2022/07/26/1113427867/amazon-one-medical-health-care.

[26] Rosie Bradbury, "Amazon is Introducing New Tech ot Monitor Shoppers in its Grocery Stores and Share Data with Advertisers," *Yahoo Finance* (June 30, 2022), https://finance.yahoo.com/news/amazon-introducing-tech-monitor-shoppers-121830994.html.

form of highly targeted ad placements."[27]

Apple, which operates one of the world's most profitable online app stores,[28] is also growing its surveillance advertising business.[29] The company plans to expand in-app advertising, push into new advertising sectors, and build out its proprietary advertising network.[30]

Beyond the largest "Big Tech" platforms, telecom operators and ISPs, other sectors of the economy are also in need of greater scrutiny for their surveillance advertising practices. Increasingly, brick and mortar retailers are expanding their e-commerce offerings, replete with in-house digital advertising operations. Such is the case with Walmart, the world's largest retailer, and its "plans to become a top 10 ad business."[31] The firm already offers a robust programmatic advertising marketplace built upon, at least in part, first-party data collected from the 90% of U.S. households that shop at Walmart each year.[32] In the health-care industry, CVS[33] and Walgreens[34] have both grown their digital advertising businesses. These plans center around leveraging first-party data about customers to generate more personalized advertising opportunities for advertisers. Even grocery chain Kroger has moved into the programmatic advertising market.[35] In addition to these examples, the so-called "consumer data and analytics industry" includes news outlets, media and publishing firms like Walt Disney, CBS, and video game publishers, as well as financial services firms, including banks, digital payment processing companies, and insurance companies.[36]

---

[27] Tech Transparency Project, "Amazon's Data Dragnet" (January 22, 2021), https://www.techtransparencyproject.org/articles/amazons-data-dragnet.
[28] Sarah Perez, "App Stores to see Record Consumer Spend of $133 Billion in 2021, 143.6 Billion New App Installs," *TechCrunch* (December 7, 2021), https://techcrunch.com/2021/12/07/app-stores-to-see-record-consumer-spend-of-133-billion-in-2021-143-6-billion-new-app-installs/.
[29] Kif Lesswing, "Apple Plans to Sell Ads in New Spots in the App Store by Year-End," *CNBC* (September 13, 2022), https://www.cnbc.com/2022/09/13/apple-plans-new-spots-for-ads-in-app-store-by-the-end-of-the-year.html.
[30] Ashley Capoot, "Apple Reportedly Plans to Put Ads in More Apps on Your iPhone," *CNBC* (August 15, 2022), https://www.cnbc.com/2022/08/15/apple-reportedly-plans-to-put-ads-in-more-apps-on-your-iphone.html.
[31] John McCarthy, "Walmart Reveals Ad Profits and Plans to Become a 'top 10 ad business,'" *The Drum* (February 18, 2022), https://www.thedrum.com/news/2022/02/18/walmart-reveals-ad-profits-and-plans-become-top-10-ad-business; Peter Adams, "Walmart Acquires Thunder Ad Tech as it Preprr Self-Serve Display Portal," *Marketing Dive* (February 4, 2021), https://www.marketingdive.com/news/walmart-acquires-thunder-ad-tech-as-it-preps-self-serve-display-portal/594538/.
[32] *Walmart*, "Walmart Connect"(last accessed September 28, 2022), https://www.walmartconnect.com/.
[33] Robert Williams, "CVS Pharmacy launches ad network for in-store, online campaigns," *Marketing Dive* (August 25, 2020), https://www.marketingdive.com/news/cvs-pharmacy-launches-ad-network-for-in-store-online-campaigns/584060/.
[34] Adrianne Pasquarelli, "Walgreens Rolls out its own Retail Media Network," *AdAge* (December 3, 2020), https://adage.com/article/cmo-strategy/walgreens-rolls-out-its-own-retail-media-network/2298531.
[35] Bridget Goldschmidt, "Kroger Debuts Private Programmatic Advertising Marketplace," *Progressive Grocer* (October, 20, 2021), https://progressivegrocer.com/kroger-debuts-private-programmatic-advertising-marketplace.
[36] *Privacy Bee*, "Who are the Largest Data Brokers?" (last accessed September, 28, 2022), https://privacybee.com/blog/these-are-the-largest-data-brokers-in-america/.

Another subset of companies operate ad exchanges, digital marketplaces where other actors (ad networks, advertisers, publishers, etc.) can buy and place ads. At a high level, these automated marketplaces function as auctions, enabling buyers to bid on designated advertising space (e.g., banner ads on a website, pop-up ads, and native ads on social media networks) encountered by users online. As one scholar explains, "These bids are typically made based on what an advertiser knows about you, the user. In this transaction, the website publisher puts the ad space up for auction, advertisers (or their ad agencies) bid on it, and intermediaries known as ad tech firms handle the details."[37]

C. The Data Broker Industry and Third-Party Data

Companies using data stemming from their own interactions with users and customers—first-party data—is one thing. Selling and purchasing such data to create large-scale data sets of consumer information—third-party data—is quite another. While data brokers predate personal computing, they now function as middlemen best thought of as critical infrastructure for commercial surveillance, including surveillance advertising.[38] When referring to the "data broker industry" we follow the Commission's own definition, generally meaning the business entities that collect and/or sell information about individuals to third parties, including businesses and government.[39]

The global data broker industry earns an estimated $200 billion yearly, and there are believed to be around 4,000 individual data broker firms, the largest of which include Acxiom, Epsilon, and Equifax.[40] Giving some sense of the scale of this surveillance, Acxiom has revealed that its data collection "encompasses more than 62 countries, 2.5 billion addressable consumers and more than 10,000 attributes—for a comprehensive representation of 68 percent of the world's online population."[41]

These firms collectively acquire and monetize information on billions of people around the world, including every conceivable kind of sensitive personal information. Of particular concern,

---

[37] Joshua A. Braun and Jessica L. Eklund, "Fake News, Real Money: Ad Tech Platforms, Profit-Driven Hoaxes, and the Business of Journalism," *Digital Journalism* (2019), Vol. 7, No. 1, 1-21, https://www.tandfonline.com/doi/pdf/10.1080/21670811.2018.1556314.

[38] Urbano Reviglio, "The Untamed and Discreet Role of Data Brokers in Surveillance Capitalism: a Transnational and Interdisciplinary Overview," *Internet Policy Review* (August 4, 2022), https://doi.org/10.14763/2022.3.1670.

[39] *Federal Trade Commission*, "Protecting consumer privacy in an era of rapid change" (FTC Report March 2012). https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[40] *WebFX*, "What are Data Brokers - and What is Your Data Worth?" (last accessed September 28, 2022), https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/

[41] *Acxiom*, "Acxiom Launches Global Data Navigator Tool Offering Marketers Visibility into Global Audiences" (May 9, 2018), https://www.acxiom.com/news/acxiom-launches-global-data-navigator-tool-offering-marketers-visibility-into-global-audiences/.

this includes data about demographics, gender, sexuality, health, religion, socio-economics, political beliefs, and even information about life events such as weddings and births.

From the sale of personal histories to tenant screening companies[42] to the sharing of information about menstrual cycles for marketing purposes,[43] there are seemingly no limits on the kinds of personal information data brokers attempt to monetize. Indeed, in a 2013 congressional testimony, the Executive Director of the World Privacy Forum, Pam Dixon, testified that data brokers had compiled lists containing the home addresses of police officers, rape survivors, domestic violence shelters, patients with genetic diseases, and others.[44]

In the absence of a federal privacy law, the industry operates virtually unchecked. Data brokers have sold personal information to hedge funds,[45] health insurance companies,[46] and law enforcement agencies.[47] The purchasing of personal information by government entities is especially concerning. As numerous reports have detailed, agencies such as the Federal Bureau of Investigation, the Department of Homeland Security, the Justice Department, and others have bought information from, and entered into contracts with, commercial data brokers.[48] In 2021, the Center for Democracy and Technology released a report on this issue, detailing how law enforcement and intelligence agencies circumvent legal requirements to acquire this information by exploiting a loophole in the Electronic Communications Privacy Act.[49] Speaking of the risks

---

[42] Lauren Kirchner, "When Zombie Data Costs You a Home," *The Markup* (October 6, 2020), https://themarkup.org/locked-out/2020/10/06/zombie-criminal-records-housing-background-checks.
[43] Natasha Lomas, "Flo Gets FTC Slap for Sharing User Data When It Promised Privacy," *TechCrunch* (January 13, 2021), https://techcrunch.com/2021/01/13/flo-gets-ftc-slap-for-sharing-user-data-when-it-promised-privacy/.
[44] Testimony of Pam Dixon Executive Director, World Privacy Forum, "What Information Do Data Brokers Have on Consumers, and How Do They Use it?," *Senate Committee on Commerce, Science, and Transportation* (December 18, 2013), https://www.worldprivacyforum.org/wp-content/uploads/2013/12/WPF_PamDixon_CongressionalTestimony_DataBrokers_2013_fs.pdf.
[45] Joseph Cox, "Leaked Document Shows How Big Companies Buy Credit Card Data on Millions of Americans," *Vice* (February 19, 2020), https://www.vice.com/en/article/jged4x/envestnet-yodlee-credit-card-bank-data-not-anonymous.
[46] Marshall Allen, "Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates," *ProPublica* (July 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates
[47] Joan Friedland, "How the Trump Deportation Machine Relies on Inaccurate Databases and Unregulated Data Collection," *National Immigration Law Center* (November 1, 2019), https://www.nilc.org/2019/11/01/inaccurate-data-unregulated-collection-fuel-deportation-machine/; Ashley Belanger, "The DHS Bought a 'Shocking Amount' of Phone-Tracking Data," *Wired* (July 28, 2022), https://www.wired.com/story/dhs-surveillance-phone-tracking-data/.
[48] Alexandra Kelley, "Democrat lawmakers addressed seven federal law enforcement agencies for documentation of how often data was procured outside formal legal channels," *Nextgov* (August 17, 2022), https://www.nextgov.com/analytics-data/2022/08/law-enforcement-purchase-consumer-data-draws-congressional-scrutiny/375979/.
[49] Carey Shenkman, Sharon Bradford Franklin, Greg Nojeim, and Dhanaraj Thakur, "Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies are Buying Your Data from Brokers," *Center for Democracy and Technology* (2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf.

involved when this information includes sensitive location data, the Brennan Center has also asserted that these practices undermine the Fourth Amendment, enable "opportunities for law enforcement monitoring that would otherwise be infeasible due to resource and technical contracts…[and facilitate] unimpeded government surveillance on a massive scale that would be have been unimaginable a few decades ago."[50] One proposed remedy for this problem is the Fourth Amendment is Not For Sale Act, a bipartisan bill introduced last year that "closes the legal loophole that allows data brokers to sell Americans' personal information to law enforcement and intelligence agencies without any court oversight…"[51] Another intervention involves strictly limiting the collection of such data in the first place through stringent data minimization, as we discuss in the Recommendations section of this comment.

Data brokers have also advertised to potential buyers troves of personal information collected about U.S. military personnel, presenting a troubling national security risk.[52] Because business deals between data brokers and their clients are opaque, and there are few restrictions on what can be sold, the public understands little about how and where this information is used.

Recently, the U.S. Government Accountability Office underscored the need for greater transparency to better protect consumers who "may not always know what data businesses are collecting about them, or how those data are used and shared." Nor are they able to stop the collection of this data or validate its accuracy.[53] Without the ability to inspect, verify, or correct information about themselves, users are subject to two kinds of data harms: 1) those stemming from accurate information and 2) those related to inaccurate information. Accurate information harms are those that occur when accurate information is used, or inferred, as part of algorithmic decision making in ways that create adverse effects. This was the experience of the plaintiffs in a 2019 lawsuit against Facebook. The suit was brought against the platform because it had allowed housing ads targeted on the basis of race, religion, and national origin, a violation of federal law.[54] Inaccurate information harms arise when the information collected or inferred about a person is false or incomplete, leading to a detrimental outcome. For example, a 2014 report by the Brennan Center on data brokers detailed how "police sometimes rely on inaccurate

---

[50] Laura Hect-Felella, "Federal Agencies are Secretly Buying Consumer Data," *The Brennan Center* (April 16, 2021), https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data.
[51] "Wyden, Paul, and Bipartisan Members of Congress Introduce the Fourth Amendment Is Not For Sale Act," *Office of Senator Ron Wyden* (April 21, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act-.
[52] Justin Sherman, "Data Brokers are Advertising Data on U.S. Military Personnel," *Lawfare Blog* (August 23, 2021), https://www.lawfareblog.com/data-brokers-are-advertising-data-us-military-personnel.
[53] "Consumer Data: Increasing USe Poses Risks to Privacy," *U.S. Government Accountability Office* (September 13, 2022), https://www.gao.gov/products/gao-22-106096.
[54] Naomi Nix and Elizabeth Dwoskin, "Justice Department and Meta Settle Landmark Housing Discrimination Case," *The Washington Post* (June 21, 2022), https://www.washingtonpost.com/technology/2022/06/21/facebook-doj-discriminatory-housing-ads/.

information [from these businesses] to supplement investigations."[55] The Electronic Privacy Information Center (EPIC) has similarly warned that data brokers "maintain information about consumers that is often inaccurate, wrongfully denying them credit, housing, or even a job."[56]

D. The Proliferating Harms of Surveillance Advertising

As we have documented, virtually every online experience is potential fodder for the surveillance advertising industry. Indeed, it is estimated that "over 90% of all digital display ad dollars will transact programmatically" in 2022.[57] Reflecting on the ubiquity of online advertising, Tim Hwang, author of a book on the subject, has noted that "[y]ou can almost take any piece of the web, from the smallest thing to the biggest thing, and basically say, 'What does the role of advertising play in shaping this?'[...] It acts on everything you see online."[58]

As more and more businesses turn toward digital advertising as a source of revenue, the scope of commercial surveillance continues to increase. In terms of total revenues, the global digital advertising market grew 14% from 2016-2021, topping out at $461 billion last year.[59] It is predicted to exceed $700 billion in 2025.[60]

Many consequences of this trend are sadly predictable. As the remainder of this comment will detail, the widespread use of commercial surveillance broadly, and surveillance advertising in particular, as detailed above, have profound negative implications for the right to privacy, free expression, civil liberties, autonomy, as well as for the agency of online users. To illustrate these dangers, we focus on two broad areas of concern: 1) the accountability gaps and the associated online harms of surveillance advertising and 2) the unique threats commercial surveillance raises for data security.

---

[55] Meghan Koushik, "Data Brokers Know a Lot About You, But What Do You Know About Them?," *Brennan Center for Justice* (October 31, 2014), https://www.brennancenter.org/our-work/analysis-opinion/data-brokers-know-lot-about-you-what-do-you-know-about-them.

[56] EPIC, "Data Brokers," *Electronic Privacy Information Center* (last accessed October 27, 2022), https://epic.org/issues/consumer-privacy/data-brokers/.

[57] Meaghan Yuen, "Programmatic Digital Display Advertising in 2022: Ad Spend, Formats, and Forecast," *Insider Intelligence* (May 23, 2022), https://www.insiderintelligence.com/insights/programmatic-digital-display-ad-spending/.

[58] As quoted in Paris Marx, "The Ads-Based Internet is About to Collapse. What Comes Next," *OneZero* (November 10, 2020), https://onezero.medium.com/the-ad-based-internet-is-about-to-collapse-what-comes-next-48e31d648a35.

[59] "Global Digital Advertising Market Almanac 2022: Total Revenues of $486 Billion in 2021 - Summary, Competitive Analysis, and Forecasts 2017-2026," *Businesswire*, (July 28, 2022), https://www.businesswire.com/news/home/20220728005533/en/Global-Digital-Advertising-Market-Almanac-2022-Total-Revenues-of-468-Billion-in-2021---Summary-Competitive-Analysis-and-Forecasts-2017-2026---ResearchAndMarkets.com.

[60] Julia Faria, "Digital Advertising in the United States - statistics & facts," *Statista* (August, 2022), https://www.statista.com/topics/1176/online-advertising/.

II. Surveillance Advertising and its Discontents

As we've noted, human rights defenders, civil society groups, and scholars—including ourselves—have long argued that many of the abuses facilitated by the digital environment stem from, or are otherwise closely connected to, targeted advertising business models. Now, consider the following examples:

- Facebook sold advertising impressions, including for ads for housing and jobs, that targeted users in a racially discriminatory manner.[61]
- Facebook allowed job advertisements on its platform that discriminated against women.[62]
- The Cambridge Analytica scandal brought to light how Facebook had violated the privacy of tens of millions of users[63] whose data was shared with third parties for political advertising and manipulation.
- YouTube illegally collected the data of children for use in its targeted advertising systems.[64]
- Google permitted a sanctioned Russian advertising technology company to access and store data about people using websites and apps in Ukraine and other parts of the world.[65]
- Google accepted and ran advertisements for firearms, some of which ran on childrens' websites, despite company policies prohibiting ads for guns.[66]
- An estimated $235 million is generated each year by ads that run on extremist and disinformation websites.[67]

The existence of such failures and abuses serves as a reminder that online advertising is a poorly regulated industry with a great capacity for public harm.

---

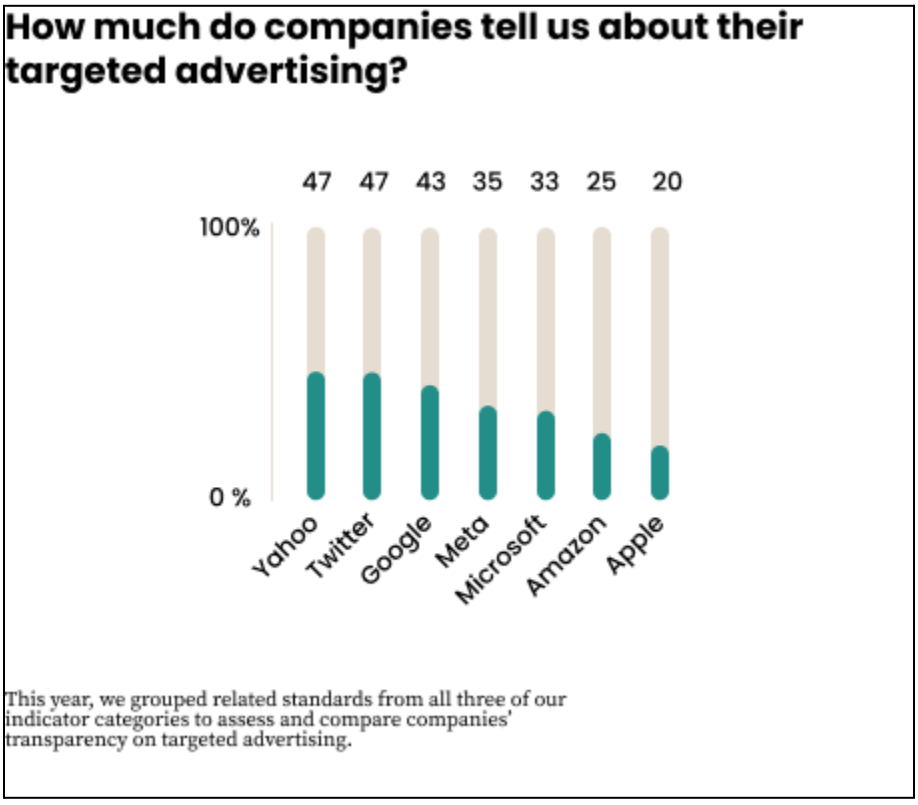
[61] Jinyan Zang, "Solving the Problem of Racially Discriminatory Advertising on Facebook," *Brookings Institution* (Oct. 19, 2021), https://www.brookings.edu/research/solving-the-problem-of-racially-discriminatory-advertising-on-facebook/.
[62] Noam Scheiber, "Facebook Accused of Allowing Bias Against Women in Job Ads," *The New York Times* (Sep. 18, 2018), https://www.nytimes.com/2018/09/18/business/economy/facebook-job-ads.html.
[63] Sam Meredith, "Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal," *CNBC* (Apr. 10, 2018), https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html.
[64] Natasha Singer and Kate Conger, "Google Is Fined $170 Million for Violating Children's Privacy on YouTube," *The New York Times* (Sept. 4, 2019), https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html.
[65] Craig Silverman, "Google Allowed a Sanctioned Russian Ad Company to Harvest User Data for Months," *ProPublica* (July 1, 2022) https://www.propublica.org/article/google-russia-rutarget-sberbank-sanctions-ukraine.
[66] Craig Silverman and Ruth Talbot, "Google Says It Bans Gun Ads. It Actually Makes Money From Them," *ProPublica* (June 14, 2022) https://www.propublica.org/article/google-guns-ads-firearms-alphabet-advertising.
[67] *Global Disinformation Index*, "Ad-funded COVID-19 Disinformation: Money, Brands, and Tech," (Mar. 1, 2020) https://www.disinformationindex.org/disinfo-ads/2020-3-1-ad-funded-covid-19-disinformation-money-brands-and-tech/.

A. Online Advertising is Poorly Governed

1. Companies' Digital Advertising Policies Lack Transparency

Advertising enforcement failures are closely related to the inadequate transparency of advertising policies. Specifically, because digital platforms refuse to share more information about their enforcement of advertising rules, the efficacy of technologies underlying these systems, or the existence and results of any human rights impact assessments diligence, the public must take these companies at their word that they have due diligence processes in place. As we will detail, the stakes are too high to hope platforms simply choose to act in the public interest. Indeed, our research reveals stark shortcomings in terms of what platforms decide to disclose publicly—including what is available for civil society groups like Ranking Digital Rights that seek to hold them accountable—about their advertising systems. Below we summarize pertinent findings from our 2022 Big Tech Scorecard for seven U.S-based companies: Amazon, Apple, Meta, Google, Microsoft, Twitter, and Yahoo.

- Overall, every company we evaluated received a failing score on our composite targeted advertising indicator. This aggregated score is an average value of our indicators that ask whether companies conduct human rights impact assessments on their targeted advertising systems and whether they clearly disclose rules around ad targeting as well as how those rules are enforced (see Fig. 1).



(Fig. 1. Composite score from all three of our indicator categories assessing and comparing U.S companies' transparency on targeted advertising.)

- Amazon, Apple, Google, Microsoft, Twitter, and Yahoo did not disclose that they assess the freedom of expression, privacy, or discrimination risks associated with their targeted advertising policies and practices.[68]
- No company disclosed that it directly notifies users about changes to its advertising content policies.[69]
- With the exception of Microsoft, which provides partial information, no company discloses that it directly notifies users about changes to advertising targeting policies.[70]
- Apple did not clarify what types of advertising content it does not permit on its iMessage and iCloud service.[71]
- Amazon did not disclose what types of targeting parameters are prohibited.[72]
- Amazon, Apple, Meta, Twitter, and Yahoo did not publish information about the total number of advertisements they restricted to enforce their advertising content policies.[73]
- Only Google and Microsoft disclosed anything about the number of advertisements they restricted to enforce advertising content and advertising targeting rules.[74]
- No company published disaggregated information about the number of advertisements that were restricted based on which advertising targeting rule was violated.[75]
- All seven companies either enabled targeted advertising by default or failed to disclose whether or not targeted advertising is switched on by default.[76]

---

[68] Ranking Digital Rights, "G4c. Impact Assessment: Targeted Advertising," *The Ranking Digital Rights Big Tech Scorecard* (last accessed October 3, 2022), https://rankingdigitalrights.org/index2022/indicators/G4c.
[69] Ranking Digital Rights, "F2b. Changes to Advertising Content Policies," *The Ranking Digital Rights Big Tech Scorecard* (last accessed October 3, 2022), https://rankingdigitalrights.org/index2022/indicators/F2b.
[70] Ranking Digital Rights, "F2c. Changes to Advertising Targeting Policies," *The Ranking Digital Rights Big Tech Scorecard* (last accessed October 3, 2022), https://rankingdigitalrights.org/index2022/indicators/F2c.
[71] Ranking Digital Rights, "F3b. Advertising Content Rules and Enforcement," *The Ranking Digital Rights Big Tech Scorecard* (last accessed October 3, 2022), https://rankingdigitalrights.org/index2022/indicators/F3b.
[72] Ranking Digital Rights, "F3c. Advertising Targeting Rules and Enforcement," *The Ranking Digital Rights Big Tech Scorecard* (last accessed October 3, 2022), https://rankingdigitalrights.org/index2022/indicators/F3c.
[73] Ranking Digital Rights, "F4c. Data About Advertising Content and Advertising Targeting Policy Enforcement, *The Ranking Digital Rights Big Tech Scorecard* (last accessed October 3, 2022), "https://rankingdigitalrights.org/index2022/indicators/F4c.
[74] Ranking Digital Rights, "F4c. Data About Advertising Content and Advertising Targeting Policy Enforcement," *The Ranking Digital Rights Big Tech Scorecard* (last accessed October 3, 2022), https://rankingdigitalrights.org/index2022/indicators/F4c.
[75] Ranking Digital Rights, "F4c. Data About Advertising Content and Advertising Targeting Policy Enforcement," *The Ranking Digital Rights Big Tech Scorecard* (last accessed October 3, 2022), https://rankingdigitalrights.org/index2022/indicators/F4c.
[76] Ranking Digital Rights, "P7. Users' Control Over their own User Information," *The Ranking Digital Rights Big Tech Scorecard* (last accessed October 3, 2022), https://rankingdigitalrights.org/index2022/indicators/P7.

- Amazon, Apple, Google, and Yahoo did not disclose whether or not users can obtain all the information that the company has inferred about them, information that is commonly used for advertising purposes.[77]

Despite detailed ad policies, vast technical resources, and a large safety and security workforce, these companies remain unwilling to disclose more information. This strongly suggests that these businesses cannot effectively govern their ad policies and want to obfuscate these failures.

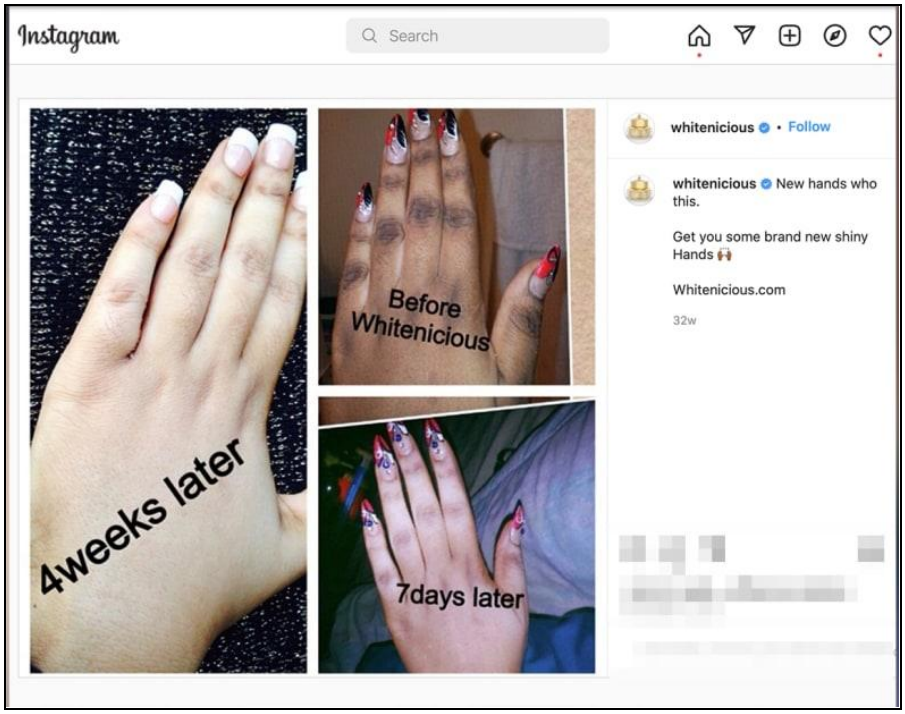
2. Digital Advertising Policies are Inadequately Enforced

Digital platforms, we know, have a particularly poor track record of governing their ad systems in a privacy-respecting manner. They cannot and should not be trusted to self-regulate. Their gaps in policy and enforcement lead to harms that fall into two (non-mutually exclusive) general categories: content policy failures—enforcement issues related to the substance of an advertisement—and targeting policy failures—-enforcement issues related to the delivery (i.e., target selection and optimization) of an advertisement.

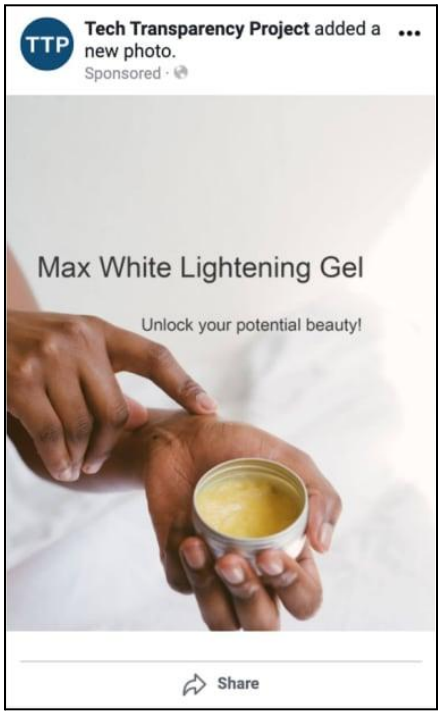
For example, in 2017, reporting revealed that Meta enabled advertisers to reach "Jew haters" via ad targeting tools.[78] In addition to misinformation and discrimination, advertisements on social media for harmful products such as skin-whitening creams, which can contain chemicals and other harmful ingredients, is another area of concern.[79] While many digital platforms claim to prohibit advertising for these dangerous "cosmetics," the enforcement of such policies leaves much to be desired. In fact, one advocacy group testing Meta's enforcement capacity was able to run a Facebook ad for skin-whitening gel targeting children, a direct violation of platform rules (see Figs. 2 and 3).

---

[77] Ranking Digital Rights, "P8. Users' Access to their Own User Information," *The Ranking Digital Rights Big Tech Scorecard* (last accessed October 3, 2022), https://rankingdigitalrights.org/index2022/indicators/P8.
[78] Julia Angwin, Madeleine Varner and Ariana Tobin, "Facebook Enabled Advertisers to Reach 'Jew Haters,'" *ProPublica* (Sept. 14, 2017), https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters.
[79] Jacqui Palumbo, "Social media is rife with skin-whitening products. But little is being done to regulate the market," *CNN* (Jun. 22, 2022) https://www.cnn.com/style/article/skin-whitening-products-social-media-as-equals-intl-cmd/index.html.



(Fig 2. "A post from Instagram advertising a skin whitening process." See fn. 79.)



(Fig. 3. "A test ad by the Tech Transparency Project that aimed to intentionally violate Meta's policies was approved by Facebook." See fn. 79.)

The U.S. Consumer Products Safety Commission (CPSC) has also raised concerns about Facebook Marketplace due to the advertisement and sale of banned and recalled products on the platform. Writing to Meta CEO Mark Zuckerberg, CPSC Chair Alex D. Hoehn-Sairc noted these products pose "a serious threat to the health and lives of consumers, including infants and toddlers…"[80]

In September 2022, Consumer Reports published an article examining the ways third-party sellers have used Meta's advertising systems to promote dangerous and illegal dietary supplements.[81]As the non-profit detailed in its report, poor governance of the Facebook advertising platform enabled the placement of ads for:

- A sleep aid containing a substance prohibited by the Food and Drug Administration;
- Comfrey, a plant containing poisonous chemicals that is illegal to sell for oral consumption in the U.S.; and
- Kraton, a substance characterized as a "drug of concern" by the Drug Enforcement Agency.

Consumer Reports identified these ads through the platform's public ad library[82] and by using The Markup's "Citizen Browser" Facebook investigation tool.[83] In response to the reporting, Meta stated that it had policies in place prohibiting the promotion of these substances. But policy without enforcement is public relations, not consumer protection. Ranking Digital Rights's efforts to engage directly with the company on issues related to advertising have been met with stonewalling. It appears that no one on Meta's public policy team is willing or able to discuss advertising policy enforcement.

3. Poor Governance Makes the Online Advertising Ecosystem Ripe for Exploitation

Due to poor governance and inadequate enforcement, the online advertising ecosystem is easily exploited by a range of bad actors, resulting in serious harms to consumers. For example, Meta has long struggled with the spread of content related to human trafficking and domestic servitude. In fact, as recently as 2018, the company had no policy against posts recruiting domestic servants. In 2019, one employee described the company's approach to the issue as

---

[80] Consumer Products Safety Commission, "Letter to Mark Zuckerberg" (July 13, 2022), https://www.cpsc.gov/s3fs-public/CPSC%20to%20Meta%20Letter%2007_13_22.pdf?VersionId=uqcldimaObNhKaYZJDbHvJYUsyx1Ju1K.

[81] Kaveh Waddell, "Marketers are Using Facebook to Promote Dangerous and Illegal Supplements," *Consumer Reports* (September 22, 2022), https://www.consumerreports.org/health/supplements/dangerous-illegal-supplements-promoted-on-facebook-a6605223059/.

[82] Meta, Ad Library (last accessed October 3, 2022), https://www.facebook.com/ads/library/.

[83] Surya Mattu, Leon Yin, Angie Waller, and Jon Keegan, "How We Built a Facebook Inspector," *The Markup* (January 5, 2021), https://themarkup.org/citizen-browser/2021/01/05/how-we-built-a-facebook-inspector.

lacking "proactive detection" strategies.[84] According to documents obtained by whistleblower Frances Haugen, in 2018 an internal investigation team found multiple domestic trafficking operations, "including one with at least 20 victims, and organizers who spent at least $152,000 on Facebook ads for massage parlors."[85]

Another harm related to surveillance advertising arises when bad actors attempt to take advantage of consumers through manipulative ads. Consider the following incidents involving teenagers:

- An internal report by Facebook revealed that the company demonstrated to advertisers its ability to identify, in real-time, when teenagers were experiencing emotional distress.[86]
- Facebook approved advertisements for alcohol, gambling, and extreme weight loss that targeted teenagers on the platform.[87]
- In an experiment conducted by staffers from Senator Richard Blumenthal's office, his team was able to place Instagram advertisements that glorified eating disorders and promoted extreme diets to accounts that had been registered as 13-year-old girls.[88] Other platforms have promoted similar ads.[89]

Other forms of fraud via advertising abound. To cite a few recent examples:

- In 2020, the Tech Transparency Project (TPP) reported on the ways that malicious actors had attempted to scam Americans out of their Covid relief funds. "TTP identified dozens of examples of Google targeting these searches [for Covid stimulus checks] with questionable ads aimed at exploiting financially distressed people. The ads direct users to

[84] Clare Duffy, "Facebook has Known it Has a Human Trafficking Problem for Years. It Still Hasn't Fully Fixed It," *CNN* (October 25, 2021), https://www.cnn.com/2021/10/25/tech/facebook-instagram-app-store-ban-human-trafficking.
[85] Justin Scheck, Newly Purnell, and Jeff Horwitz, "Facebook Employees Flag Drug Cartels and Human Traffickers. The Company's Response is Weak, Documents Show," *The Wall Street Journal* (September 16, 2021), https://www.wsj.com/articles/facebook-drug-cartels-human-traffickers-response-is-weak-documents-11631812953.
[86] Sam Levin, "Facebook Tolk 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.
[87] Kaveh Waddell, "Facebook Approved Alcohol and Gambling Ads Targeting Teens," *Consumer Reports* (July 27, 2021), https://www.consumerreports.org/advertising-marketing/facebook-approved-alcohol-gambling-tobacco-weight-loss-ads-targeting-teens-a1062200831/.
[88] Donnie O'Sullivan, Clare Duffy, and Sarah Jorgensen, "Instagram Promoted Pages Glorifying Eating Disorders to Teen Accounts," *CNN* (October 4, 2021), https://www.cnn.com/2021/10/04/tech/instagram-facebook-eating-disorders/index.html.
[89] Brit Dawson, "Eating Disorder Sufferers on the Danger of Weight Loss Ads on TikTok," *Dazed Digital*, (September 25, 2020), https://www.dazeddigital.com/life-culture/article/50566/1/eating-disorder-sufferers-on-the-danger-of-weight-loss-ads-on-tiktok.

sites that charge bogus fees for stimulus money, try to harvest people's personal data, or plant unwanted software into their web browsers."[90]

- Also in 2020, TPP reported that they had "found that search terms like 'register to vote,' 'vote by mail,' and 'where is my polling place' generated ads linking to websites that charge bogus fees for voter registration, harvest user data, or plant unwanted software on people's browsers."[91]
- Cybersecurity firm Check Point documented, in 2021, that scammers were using Google Ads to steal cryptocurrencies. An estimated $500,000 of crypto was stolen via ads and phishing websites.[92]
- In 2021, reporters documented ads impersonating U.S. government officials in paid Google search results.[93]
- In 2022, Google was found to be displaying misleading advertisements about abortions, directing people seeking information about the procedure to sites with innacurate medical information.[94]

B. The Harms Associated with Surveillance Advertising are Systemic

Focusing on commercial surveillance risks that stem from poor enforcement, inadequate transparency practices, and overall weak governance mechanisms is a helpful starting point. However, many of the risks associated with the practice are systematic, or structural, in nature. In this sense, systemic harms are those produced by social, economic, historical, and political forces, and then reinforced through surveillance advertising practices. As some scholars have noted, structural "harms are not always recognizable through conventional causation and intent parameters of legal liability,"[95] which can result in their exclusion from standard legal remedies. In this section we focus on two forms of structural harms: Privacy harms[96] and algorithmic bias and discrimination.

---

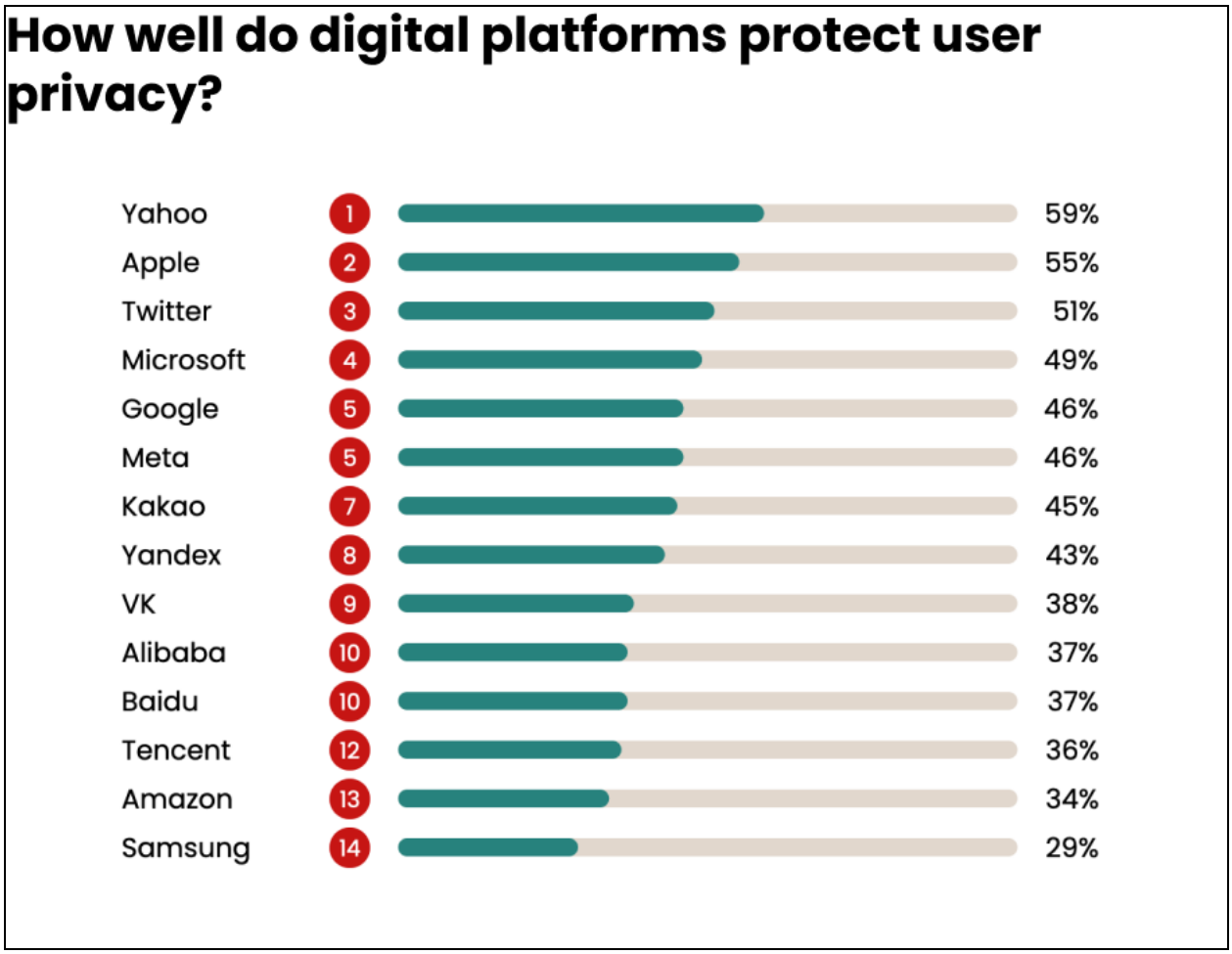
[90] "Google Helps Scammers Target American Seeking Stimulus Checks," *Tech Transparency Project* (June 16, 2020), https://www.techtransparencyproject.org/articles/google-helps-scammers-target-americans-seeking-stimulus-checks.
[91] "Google Pushing Scam Ads on Americans Searching for How to Vote," *Tech Transparency Project* (June 29, 2020), https://www.techtransparencyproject.org/articles/google-pushing-scam-ads-americans-searching-how-vote.
[92] "Scammers Used google Ads to Steal ~$500k Worth of Cryptocurrency," *Check Point* (November 4, 2021), https://blog.checkpoint.com/2021/11/04/scammers-used-google-ads-to-steal-500k-worth-of-cryptocurrency/.
[93] Jeremy B. Merrill, "Ads Are Impersonating Government Websites in Google Results, Despite Ban," *The Markup* (May 13, 2021), https://themarkup.org/google-the-giant/2021/05/13/ads-are-impersonating-government-websites-in-google-results-despite-ban.
[94] Rachel Schraer, "Anti-aboriton Groups Target Women with Misleading Ads," *BBC News* (May 17, 2022), https://www.bbc.com/news/health-61320202; Imad Khan, "Google Ads Still Linking to Misleading Info in Abortion Searches," *CNET* (September 29, 2022), https://www.cnet.com/news/politics/google-ads-still-linking-to-misleading-info-in-abortion-searches/.
[95] Kebene Wodajo, "Mapping (In)visibility and Structural Injustice in the Digital Space," *Journal of Responsible Technology*, Vol 9, (April 2022), https://doi.org/10.1016/j.jrt.2022.100024.
[96] Danielle Keats Citron and Daniel J. Solove. "Privacy harms." *BU L Rev.* 102 (2022): 793. https://ssrn.com/abstract=3782222.

1. Privacy Harms

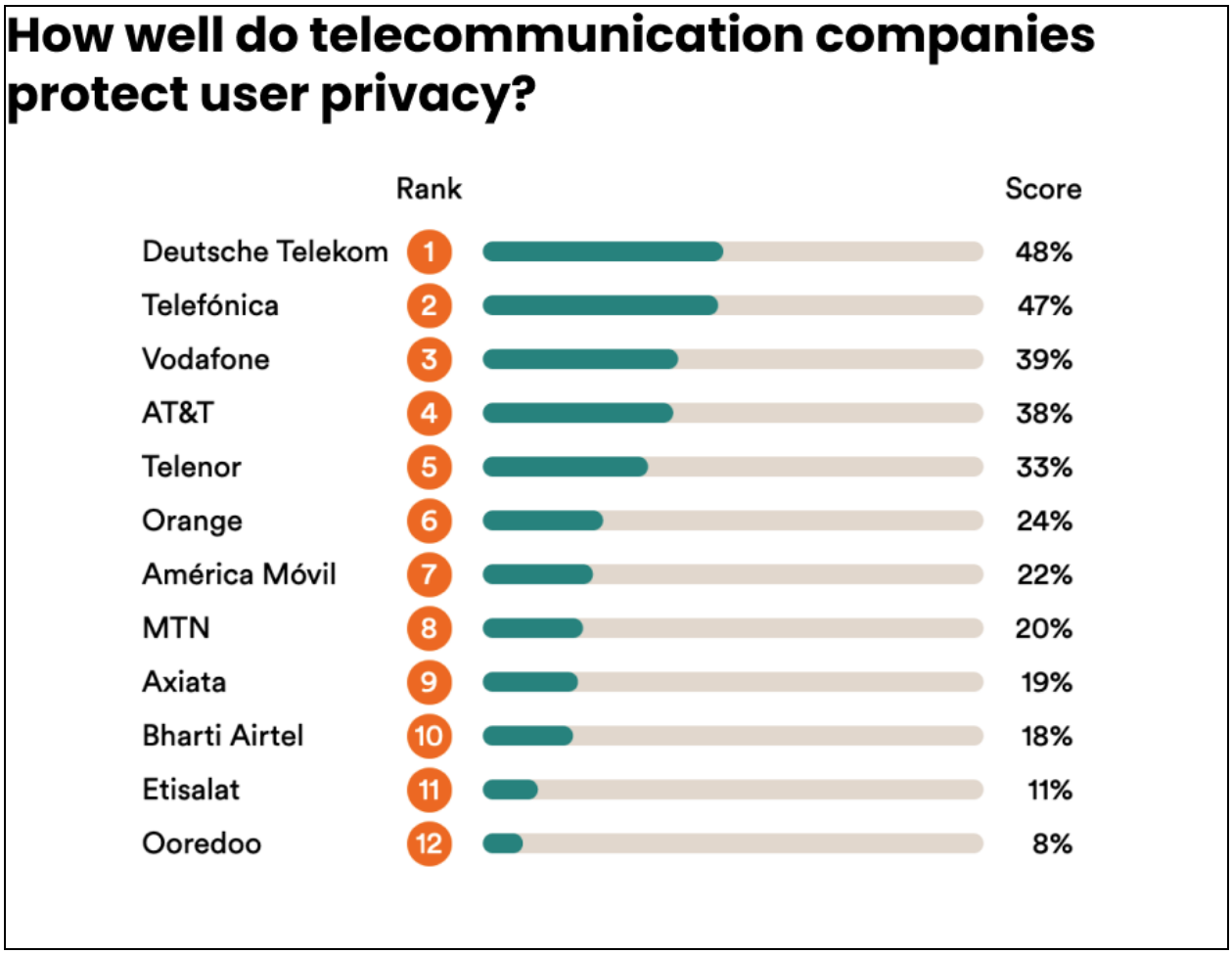
Among the most pressing issues related to the digital advertising industry is the lack of meaningful consumer privacy safeguards. As media scholar Sarah Myers West (now an advisor to FTC Chair Lina Khan) has underscored, an entire sector of the economy is "premised on the collection and commoditization of user data—one in which user privacy is the price of entry for all online experiences…"[97] Indeed, there can be no ad targeting without surveillance.[98]

According to our research, Internet and communication technology firms fall far short in protecting user privacy. In both our analyses of digital platforms in 2022 (see fig. 4)[99] and of telecommunications companies in 2021 (see fig. 5),[100] not one company received a passing score on our privacy indicators.

[97] Sarah Myers West, "Data Capitalism: Redefining the Logics of Surveillance and Privacy," *Business & Society* Volume 58, Issue 1 at 20 (January, 2019), https://doi.org/10.1177/0007650317718185.
[98] Nathalie Maréchal and Ellery Roberts Biddle, "It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge," *New America* (March 17, 2020), https://www.newamerica.org/oti/reports/its-not-just-content-its-business-mode; Jeff Gary and Ashkan Soltani, "First Things First: Online Advertising Practices and their Effects on Platform Speech," *The Knight First Amendment Institute at Columbia University* (August 21, 2019), https://knightcolumbia.org/content/first-things-first-online-advertising-practices-and-their-effects-on-platform-speech.
[99] Ranking Digital Rights, "Data Explorer" (last accessed Jul. 25, 2022), https://rankingdigitalrights.org/index2022/explore.
[100] Ranking Digital Rights, "The 2020 RDR Index" (last accessed Jul. 25, 2022), https://rankingdigitalrights.org/index2020/.



(Figure 4. The average score each digital platform received for our privacy indicators in 2022. This category measures how well companies respect the right to privacy of users, as articulated in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and other international human rights instruments.)



(Figure 5. The average score each telecommunication company received for our privacy indicators in 2021. This category measures how well companies respect the right to privacy of users, as articulated in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and other international human rights instruments.)

The FTC's own research has also documented behavior from ICT firms that undermines user privacy.[101] Verizon, for example, used a "supercookie" technology to track consumers' activity across the web in order to sell data to advertisers.[102] And, as the Commission's fine against Twitter just this year for misusing user phone data—originally collected for multi-factor

[101] Federal Trade Commission, "A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers" (Oct. 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.
[102] Jacob Kastrenakaes, "FCC Fines Verizon $1.35 Million Over 'Supercookie' Tracking," *The Verge* (March 7, 2016), https://www.theverge.com/2016/3/7/11173010/verizon-supercookie-fine-1-3-million-fcc.

authentication—for advertising purposes indicates, privacy violations from digital platforms are also widespread.[103]

2. *Algorithmic Bias and Discrimination*
(Responds to ANPR Q. 65; Q. 66)

In order to deliver targeted advertisements, companies rely upon algorithmic systems with well-established flaws related to bias and discrimination. These problems have been widely documented by civil society groups and academic researchers.[104] It bears noting that the consequences of these technologies disproportionately burden marginalized communities.[105] Prior to joining the FTC, Commissioner Alvaro Bedoya argued that the burdens of surveillance technologies—a key element of targeted advertising[106]—fall "overwhelmingly on the shoulders of immigrants, heretics, people of color, the poor, and anyone else considered 'other.'"[107] Studies show that targeted advertisements can lead to housing discrimination on the basis of race[108] and employment discrimination on the basis of gender.[109] Other research has examined how, for

---

[103] "FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads," *Federal Trade Commission* (May 25, 2022) https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

[104] Latanya Sweeney, "Discrimination in Online Ad Delivery," *Communications of the ACM* (2013), https://dl.acm.org/doi/pdf/10.1145/2460276.2460278; Diego Naranjo & Jan Penfrat, "Surveillance-based Advertising: An Industry Broken by Design and by Default," *European Digital Rights* (Mar. 9, 2021), https://edri.org/our-work/surveillance-based-advertising-an-industry-broken-by-design-and-by-default/l; Bennett Cyphers & Adam Schwartz, "Ban Online Behavioral Advertising," *Electronic Frontier Foundation* (Mar. 21, 2022), https://www.eff.org/deeplinks/2022/03/ban-online-behavioral-advertising; Sarah Meyers West, "Data Capitalism: Redefining the Logics of Surveillance and Privacy," *Business & Society (2019)*, 58(1), pp. 20–41. doi: 10.1177/0007650317718185; Safiya Noble, "Algorithms of Oppression: Data Discrimination in the Digital Age," *New York University Press* (2016). New York: New York.

[105] "Human Rights in the Age of Artificial Intelligence," Access Now (Nov. 2018), https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf.

[106] *See* Nathalie Maréchal, Rebecca MacKinnon, Jessica Dheere, "Getting to the Source of Infodemics: It's the Business Model" Ranking Digital Rights (last updated May 27, 2020), https://www.newamerica.org/oti/reports/getting-to-the-source-of-infodemics-its-the-business-model/by-protecting-data-federal-privacy-law-can-reduce-algorithmic-targeting-and-the-spread-of-disinformation ("The data that is collected [by online surveillance technologies] becomes the core ingredient for developing very powerful digital profiles about users that can then be used by advertisers and political operatives to target groups and individuals").

[107] Alvaro Bedoya, "Privacy as Civil Right," 50 N.M. L. Rev. No. 3, 301 (2020), https://ssrn.com/abstract=3599201.

[108] *See* Nathalie Maréchal, Ellery Roberts Biddle, "Who Gets Targeted—Or Excluded—By Ad Systems?," *Ranking Digital Rights* (last updated Mar. 17, 2020), https://www.newamerica.org/oti/reports/its-not-just-content-its-business-model/who-gets-targetedor-excludedby-ad-systems (showing that Facebook took 15 minutes to approve housing ads that were targeted to exclude African African-American, Asian-American or Hispanic people); *see also* Jinyan Zang, "Solving the Problem of Racially Discriminatory Advertising on Facebook," *Brookings Institution* (Oct. 19, 2021), https://www.brookings.edu/research/solving-the-problem-of-racially-discriminatory-advertising-on-facebook/.

[109] Matt O'Brien & Barbara Ortutay, "Study: Facebook Delivers Biased Job Ads, Skewed by Gender," *AP News* (April 20, 2021), https://apnews.com/article/discrimination-f62160cbbad4d72ce5250e6ef2222f5e; Anja Lambrecht & Catherine Tucker, "Algorithmic Bias? An Empirical Study of Apparent Gender-Based Discrimination in the Display of STEM Career Ads," *Management Science* 65, no. 7 (Jul. 1, 2019): 2966–81,

example, Meta's advertising optimization tools (the mechanisms by which advertisers set outcomes for an advertisement, such as clicks, impressions, or sales) produce "skewed, and potentially discriminatory, outcomes."[110] The authors of this study note that because discrimination in ad delivery can occur "independently from ad targeting" (i.e., the selection of ad audiences), restrictions on ad targeting cannot address the full range of discrimination resulting from digital advertising practices. In other words, discriminatory ad delivery is possible even when ads are not specifically targeted to a discrete category, because Facebook algorithmically optimizes ad delivery based on a number of competing objectives and data sources. This means that the platform may be inferring sensitive categories of information about users (e.g., race, gender, health status, or religion) based on correlations among users that share similar non-sensitive attributes such as geolocation data and other interest attributes (e.g., favorite sports teams, shopping habits, musical taste) as part of its optimization process for ad delivery.[111]

While many studies on the discriminatory harms of targeted advertisements have focused on digital platform companies,[112] internet service providers (ISPs) are also responsible for discrimination in ad targeting. For example, T-Mobile has touted its targeted advertisements product, App Insights, which enables targeting based on LGBTQ identity.[113]

---

https://pubsonline.informs.org/doi/abs/10.1287/mnsc.2018.3093; Jeremy B. Merrill, "Google Has Been Allowing Advertisers to Exclude Nonbinary People from Seeing Job Ads," *The Markup* (February 11, 2021), https://themarkup.org/google-the-giant/2021/02/11/google-has-been-allowing-advertisers-to-exclude-nonbinary-people-from-seeing-job-ads; Noam Scheiber, "Facebook Accused of Allowing Bias Against Women in Job Ads," The *New York Times* (Sep. 18, 2018), https://www.nytimes.com/2018/09/18/business/economy/facebook-job-ads.html. Although gender is not one of the protected classes in 47 U.S.C.A. § 1754(b)(1), the fact that targeted ads discriminate on the basis of gender indicates they may discriminate on the basis of other classes.

[110] Muhammad Ali et al., "Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes," *Proceedings of the ACM on Human-Computer Interaction* (Nov. 2019). https://dl.acm.org/doi/abs/10.1145/3359301

[111] Till Speicher, Muhammad Ali, Giridhari Venkatadri, Filipe Nunes Ribeiro, George Arvanitakis, Fabrício Benevenuto, Krishna P. Gummadi, Patrick Loiseau, and Alan Mislove, "Potential for discrimination in online targeted advertising," *Proceedings of Machine Learning Research* (2018), http://proceedings.mlr.press/v81/speicher18a/speicher18a.pdf.

[112] *See, e.g.*, Nathalie Maréchal, Ellery Roberts Biddle, "Who Gets Targeted—Or Excluded—By Ad Systems?," *Ranking Digital Rights* (last updated Mar. 17, 2020), https://www.newamerica.org/oti/reports/its-not-just-content-its-business-model/who-gets-targetedor-excludedby-ad-systems; Matt O'Brien & Barbara Ortutay, "Study: Facebook Delivers Biased Job Ads, Skewed by Gender," AP News (Apr. 20, 2021), https://apnews.com/article/discrimination-f62160cbbad4d72ce5250e6ef2222f5e.

[113] Shoshana Wodinsky, "Of Course T-Mobile Is Being Shady With Your App Downloads and Browsing History," *Gizmodo* (June 23, 2022), https://gizmodo.com/t-mobile-app-insights-download-history-web-browsing-adv-1849099320.

III. Data Security

(Responds to ANPR Q. 32)

It is axiomatic that the commercial surveillance industry is fueled by data. Surveillance advertising, in particular, requires a ceaseless stream of personal information in order to be effective, or so the industry claims. While figures about the amount of user data collected are hard to find, the data broker industry's astounding growth, in terms of gross revenue and new businesses, indicate the scope of commercial surveillance has increased significantly. Yet the endless collection of consumer information greatly exacerbates data security risks, including those posed by data breaches and those related to the inappropriate use and governance of personal information. These problems exist alongside the digital commercial surveillance issues detailed above and further contribute to an exploitative, privacy-infringing, and harm-filled consumer environment.

A. Companies' Data Security Practices Lack Transparency

Unfortunately, our research reveals that, as with their digital ad policies, Big Tech companies don't share as much as they should about their data security practices. Our expectations are straightforward: Companies should explain their institutional processes to ensure the security of their products and services, address security vulnerabilities when they are discovered, disclose their processes for responding to data breaches, encrypt user communications and content both in transit and at rest, and help users keep their accounts secure.

- The e-commerce platform of Amazon does not disclose that it has systems in place to limit and monitor employee access to user information, does not clearly disclose that it has a security team that conducts security audits on the company's products and services, and does not clearly disclose that it commissions third-party security audits on its products and services.[114]
- Yahoo and Apple were the only companies to receive passing marks on our indicator evaluating disclosure of information about processes for responding to data breaches.[115]
- Neither Amazon, Google, nor Twitter disclose: 1) that they will notify the relevant authorities without delay when a data breach occurs, 2) their processes for notifying data subjects who might be affected by a data breach, or 3) what kinds of steps they take to address the impact of data breaches on users.[116]

[114] Ranking Digital Rights, "P13. Security Oversight." *The Ranking Digital Rights Big Tech Scorecard* (last accessed October 5, 2022), https://rankingdigitalrights.org/index2022/indicators/P13.
[115] Ranking Digital Rights, "P15. Data Breaches." *The Ranking Digital Rights Big Tech Scorecard* (last accessed October 5, 2022), https://rankingdigitalrights.org/index2022/indicators/P15.
[116] Ranking Digital Rights, "P15. Data Breaches." *The Ranking Digital Rights Big Tech Scorecard* (last accessed October 5, 2022), https://rankingdigitalrights.org/index2022/indicators/P15.

B. Inadequate Governance and Use of Personal Information

In addition to inadequate data security transparency, digital platforms have a history of inappropriately managing and using personal information.

For example, in 2014, reporting revealed that ride-share platform Uber operated a "God View" of users on its service, allowing company employees and others to see, in real time, "all of the Ubers in a city and the silhouettes of waiting Uber users who [had] flagged cars."[117] That same year, it came to light that Uber executives were improperly accessing the logs of users' Uber trips.'[118] These issues were central to FTC's allegations that the company made deceptive privacy and data security claims. Uber settled this complaint in 2017.[119]

Amazon has also been accused of harmful data security protocols. In 2018, the company fired an employee for sharing customer email addresses with a third party.[120] Then, in 2020, Amazon fired multiple staff for sharing customer email addresses and phone numbers with third parties.[121] That same year, Amazon fired employees of its Ring camera division for accessing the live video feeds of Ring customers beyond "what was necessary for their job functions."[122]

The above examples illustrate discrete instances of inappropriate use of personal information. However, these issues commonly arise in Big Tech companies due to more systemic failures related to their data governance practices.

Based on more recent reporting about Amazon, it appears that the inappropriate accessing of customers' information is a feature, not a bug, of the company's operations. In an expansive report by *Wired* in 2021, the outlet revealed a shocking lack of protocols for securing user data, with "former Amazon chief information security officer Gary Gagnon call[ing] it, a 'free-for-all'

[117] Kashmir Hill, "'God View': Uber Allegedly Stalked USers for Party-Goers' Viewing Pleasure (Updated)," *Forbes* (October 3, 2014), https://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure/?sh=1c43a8033141.
[118] Johana Bhuiyan and Charlie Warzel, "'God View': Uber Investigates Its Top New York Executive For Privacy Violations," *Buzzfeed News* (November 18, 2014), https://www.buzzfeednews.com/article/johanabhuiyan/uber-is-investigating-its-top-new-york-executive-for-privacy.
[119] Federal Trade Commission, "Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims" (August 15, 2017), https://www.ftc.gov/news-events/news/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data-security-claims.
[120] Laura Stevens, "Amazon Fires Employee for Sharing Customer Emails," *The Wall Street Journal* (October 5, 2018), https://www.wsj.com/articles/amazon-says-third-party-seller-got-some-customers-email-addresses-1538772883.
[121] Annie Palmer, "Amazon Fires Employees for Leaking Customer Email Addresses and Phone Numbers," *CNBC* (January 11, 2020), https://www.cnbc.com/2020/01/11/amazon-fires-employees-for-leaking-customer-email-addresses-and-phone-numbers.html.
[122] Annie Palmer, "Amazon's Ring Fired Four Employees for Peeping into Customer Video Feeds," *CNBC* (January 9, 2020), https://www.cnbc.com/2020/01/09/ring-fired-four-employees-for-watching-customer-video-feeds.html.

of internal access to customer information…"[123] Subsequent reporting on Amazon whistleblowers expanded on these concerns, noting that it would be virtually "impossible" for anyone in the company to locate "all of the places where your data resides within their system," nor would they know the full scope of data collected about an individual or whether this data was adequately protected.[124]

Meta faces similar problems. In 2022, leaked internal documents revealed that the company does "not have an adequate level of control and explainability over how [its] systems use data, and thus [it] can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[125]

Twitter has also struggled to govern and protect the personal information it collects about users. In a joint complaint filed with the Securities and Exchange Commission (SEC), Department of Justice (DOJ), and FTC, a company whistleblower alleged that Twitter executives made "false and repeated statements to users and the FTC about…the Twitter platform's security, privacy, and integrity."[126] Other alleged data security failures at the company included poor internal governance over "access to core company software," and weak protocols for safeguarding the platform from hacks and spam.

According to recent statistics, more than 159 million Americans subscribe to Amazon Prime,[127] roughly 229 million Americans use Meta's Facebook platform,[128] and more than 76 million use Twitter.[129] An estimated 119 million Americans have used ride-sharing apps, with Uber being the most popular service.[130]

Although we've focused on just four companies, a majority of Americans use their services. The unfortunate reality is there are few remedies for those who wish to better protect their personal

---

[123] Will Evans, "Amazon's Dark Secret: It Has Failed to Protect Your Data," *Wired* (November 18, 2021), https://www.wired.com/story/amazon-failed-to-protect-your-data-investigation/.
[124] Vincent Manancourt, "'Millions of People's Data is at Risk' - Amazon Insiders Sound Alarm Over Security," *Politico EU* (February 24, 2021), https://www.politico.eu/article/data-at-risk-amazon-security-threat/.
[125] Lorenzo Franceschi-Biccierai, "Facebook Doesn't Know What It Does With Your Data, or Where It Goes: Leaked Document," *Vice* (April 26, 2022), https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.
[126] Joseph Menn, Elizabeth Dwoskin, and Cat Zakrzewski, "Former Security Chief Claims Twitter Buried 'Egregious Deficiencies,'" *The Washington Post* (August, 23, 2022), https://www.washingtonpost.com/technology/interactive/2022/twitter-whistleblower-sec-spam/?document=undefined.
[127] Daniela Coppola, "Number of U.S. Amazon Prime Users 2017-2025," *Statistica* (July 5, 2022), https://www.statista.com/statistics/504687/number-of-amazon-prime-subscription-households-usa/.
[128] John Gramlich, "10 Facts About Americans and Facebook," *Pew Research Center* (June 1, 2021), https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/.
[129] Meltem Odabaş, "10 Facts About Americans and Twitter," *Pew Research Center* (May 5, 2022), https://www.pewresearch.org/fact-tank/2022/05/05/10-facts-about-americans-and-twitter/.
[130] Jingjing Jiang, "More Americans are Using Ride-Hailing Apps," *Pew Research Center* (January 4, 2019), https://www.pewresearch.org/fact-tank/2019/01/04/more-americans-are-using-ride-hailing-apps/.

information from corporate inadequacies and malfeasance. At the same time, consumers are increasingly concerned about their privacy.[131] The scale and scope of the risks involved, as well as the public's broad support for privacy reform,[132] demand greater government action in this area.

IV. Recommendations for Rulemaking

(Responds to ANPR Q. 10; Qs. 43-44; Q. 46; Q. 67; Q. 73; Q. 76; Q. 83; Q. 85; Q. 89; Q. 90; Q. 92)

As we've detailed here, commercial surveillance, including that which is conducted in service of targeted advertising, harms consumers in myriad ways. The lack of regulation also impedes the growth of alternative, privacy-respecting business models. Ranking Digital Rights urges the Commission to use its authority to regulate commercial surveillance and ultimately abolish surveillance advertising. While doing so, it must also recognize that the path ahead is fraught with political and legal uncertainty. Not least among this uncertainty is the future of the American Data and Privacy Protection Act (ADPPA). The Commission should not let the perfect be the enemy of the good, nor should it be unnecessarily timid in its ambition to protect consumers.

A. The FTC Should Regulate Commercial Surveillance as an Unfair Trade Practice—Thus *De Facto* Banning Surveillance Advertising

Today's targeted advertising practices—and the invasive surveillance techniques that fuel them—routinely violate internet users' privacy rights. There is an emerging global consensus that targeted advertisements should be banned or restricted. For example, in the Digital Services Act, the European Union recently banned targeted advertisements based on certain sensitive data[133] and required disclosures for targeted ads based on other data.[134] Proposed U.S. federal legislation, the ADPPA, bans targeted advertisements based on sensitive data[135] and requires companies to honor consumers' unified opt-out of targeted advertisements based on other

---

[131] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," *Pew Research Center* (November, 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[132] Chris Teale, "Voters Overwhelmingly Back Major Provisions of Proposed Federal Data Privacy Law," *Morning Consult* (June 15, 2022), https://morningconsult.com/2022/06/15/support-for-federal-data-privacy-law/.

[133] Digital Services Act, Eur. Parl. Doc. P9_TA(2022)0269, Article 24(3) (July 5, 2022), https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_EN.pdf.

[134] Digital Services Act, Eur. Parl. Doc. P9_TA(2022)0269, Article 24(1)(c) (July 5, 2022), https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_EN.pdf.

[135] American Data Privacy and Protection Act, 117th Cong. § 102(2) (2022), https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-117-8152-P000034-Amdt-1.pdf (only allowing the processing of "sensitive covered data" for certain express purposes, which do not include targeted advertising, defined at § 101(b)(17)).

personally-identifiable data.[136] Other proposed U.S. federal legislation bans targeted advertising entirely.[137]

Earlier this year, our colleagues at Accountable Tech submitted a petition for rulemaking to the FTC, requesting that the practice be banned as an unfair trade practice.[138] Ranking Digital Rights endorsed the petition, arguing that "the surveillance advertising business model is inherently at odds with civil and human rights, liberal democracy, and the public interest."[139]

While even modest regulation would be preferable to the status quo, Ranking Digital Rights unreservedly supports a *de facto* ban on surveillance advertising, structured as strict limits on data collection and processing. Given how prevalent and lucrative it is, ending surveillance advertising and its resulting harms will require regulatory interventions and the creation of governance and accountability mechanisms throughout the advertising value chain.

B. Move Beyond Flawed "Notice and Consent" Frameworks

Much has been written about the shortcomings of so-called "Notice and Consent" frameworks, also known as "Notice and Choice," which put the onus on consumers to read and understand complex privacy policies and legal notices prior to choosing among competing providers of a given service—for example, choosing between Apple Music and Spotify on the basis of their respective data policies and practices. Setting aside the lack of meaningful competition in many subsectors of the online economy, research has shown that consumers do not read these documents[140] because they are too long,[141] too confusing,[142] and too difficult to understand.[143]

---

[136] American Data Privacy and Protection Act, 117th Cong. § 204(c) (2022), (2022),https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-117-8152-P000034-Amdt-1.pdf.
[137] Banning Surveillance Advertising Act, H.R. 6416, 117th Cong. (2022).
[138] Accountable Tech, "Petition for Rulemaking by Accountable Tech," 86 Fed. Reg. 73206 (Dec. 27, 2021), https://downloads.regulations.gov/FTC-2021-0070-0001/content.pdf.
[139] Ranking Digital Rights, "Comment in Support of Accountable Tech's Rulemaking Petition to Ban Surveillance Advertising" (Jan. 26, 2022), https://downloads.regulations.gov/FTC-2021-0070-0019/attachment_1.pdf.
[140] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," *Pew Research Center* (November 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/.
[141] Aleecia M. McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society* (2008), https://kb.osu.edu/bitstream/handle/1811/72839/1/ISJLP_V4N3_543.pdf.
[142] Lior Strahilevitz and Matthew Kugler, "Is Privacy Policy Language Irrelevant to Consumers?," *Coase-Sandor Working Paper Series in Law and Economics*, No. 776, Coase-Sandor Institute for Law and Economics, University of Chicago Law School (2016), https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2465&context=law_and_economics.
Ryan Calo, "Against Notice Skepticism in Privacy (and Elsewhere)," *University of Notre Dame Law Review,* No 87, 1027 (2012), https://scholarship.law.nd.edu/ndlr/vol87/iss3/3/.
[143] Kevin Litman-Navarro, "We Read 150 Privacy Policies. They were an Incomprehensible Disaster," *The New York Times* (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

The Commission must take into account how terms of service and privacy policies may be discriminatory in effect, both with respect to their substance and because they are so hard to understand that only a privileged subset of the population can provide truly informed consent. Moreover, these frameworks require consumers to "consent" to practices that are highly likely to violate their privacy rights, subject them to opaque and unaccountable discrimination, and put them at risk of other harms that may be difficult or even impossible for them to foresee. As legal scholar Ari Ezra Waldman argues, "there are downstream uses of data that are simply unknowable to us at the time of consent."[144]

This is not to say that consent has no place in a twenty-first century privacy framework. Our point is that consumers should not be asked to consent to practices that will harm them, or in contexts where there is an inherent power imbalance that renders their consent meaningless. Rather, companies should seek consent prior to collecting, using, or sharing data for a permissible purpose, while respecting the principles of data minimization and purpose limitation and offering the same services to all users, regardless of whether they consent to optional data collection.

C. Establish Standards for Data Minimization and Purpose Limitation

Data minimization and purpose limitation are foundational elements of contemporary privacy law.[145] Data minimization requires that personal data must only be collected, processed, or shared for explicit, permissible uses that are directly relevant and necessary to accomplish a specified purpose requested by a consumer (see next session). Purpose limitation stipulates that data collected for one purpose cannot be used for another, unrelated purpose without the consent of the data subject. The status quo, in which companies collect an inordinate amount of user data for various purposes, leaves consumers vulnerable to civil rights and data security harms. We refer the Commission to the work of our colleagues at Consumer Reports and EPIC on mandating data minimization through a Section 5 Unfairness Rulemaking.[146]

Tom Calver and Joe Miller, "Social Site Terms Tougher than Dickens," *BBC News* (July 6, 2018), https://www.bbc.com/news/business-44599968.
The Literacy Project, "Illiteracy by the Numbers" (last accessed March 7, 2022), https://literacyproj.org/.

[144] Ari Ezra Waldman, "Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power," at 56, *Cambridge University Press*, 2021.

[145] *See, e.g.*, "Guide to the General Data Protection Regulation (GDPR): The Principles," Information Commissioner's Office (last accessed May 31, 2022), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/.

[146] EPIC, "How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking," *Electronic Privacy Information Center* (Jan. 26, 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.

D. Specify Permissible Purposes for Data Collection, Use and Sharing

The principles of data minimization and purpose limitation both hinge on defining permissible and impermissible purposes for data collection, use, and sharing. Our recommendations are largely congruent with the ADPPA, with one key exception: We urge the FTC to prohibit all surveillance-based targeted advertising, whereas the ADPPA would only apply such a prohibition to children and teens up to age 17. *Text in italics denotes departures from the ADPPA.*

Covered entities should be barred from collecting, using, or transferring covered data beyond what is reasonably necessary and proportionate to provide a service requested by the individual, unless the collection, use, or disclosure would be necessary and proportionate to one of sixteen permissible purposes:

1) To initiate, manage, or complete a transaction or fulfill an order for specific products or services requested by an individual, including any associated routine administrative, operational, and account-serving activity such as billing, shipping, delivery, storage, and accounting.

2) To perform system maintenance or diagnostics; to develop, maintain, repair, or enhance a product or service for which such data was collected; to conduct internal research or analytics to improve a product or service for which such data was collected; to perform inventory management or reasonable network management; to protect against spam; to debug or repair errors that impair the functionality of a service or product for which such data was collected.

3) To authenticate users of a product or service.

4) To fulfill a product or service warranty.

5) To prevent, detect, protect against, or respond to a security incident. (Security is defined as network security, physical security, and life safety, including an intrusion or trespass, medical alerts, fire alarms, and access control security.)

6) To prevent, detect, protect against, or respond to fraud, harassment, or illegal activity. (Illegal activity means a violation of a Federal, State, or local law punishable as a felony or misdemeanor that can directly harm.)

7) To comply with a legal obligation imposed by Federal, Tribal, local, or State law, or to investigate, establish, prepare for, exercise, or defend legal claims involving the covered entity or service provider. *Sharing data with law enforcement without a court order or the explicit opt-in consent of the affected individual should be disallowed.*

8) To prevent an individual, or group of individuals, from suffering harm where the covered entity or service provider believes in good faith that the individual, or group of individuals, is at risk of death, serious physical injury, or other serious health risk.

9) To effectuate a product recall pursuant to Federal or State law.

10) To conduct a public or peer-reviewed scientific, historical, or statistical research project that is in the public interest and adheres to all relevant laws and regulations regarding such research, including regulations for the protection of human subjects, or is excluded from criteria of the institutional review board. The Commission should issue guidelines to help covered entities ensure the privacy of affected users and the security of covered data.

11) To deliver a communication that is not an advertisement to an individual, if the communication is reasonably anticipated by the individual within the context of the individual's interactions with the covered entity.

12) To deliver a communication at the direction of an individual between such individual and one or more individuals or entities.

13) To transfer assets to a third party in the context of a merger, acquisition, bankruptcy, or similar transaction when the third party assumes control, in whole or in part, of the covered entity's assets, only if the covered entity, in a reasonable time prior to such transfer, provides each affected individual with (a) a notice describing such transfer, including the name of the entity or entities receiving the individual's covered data and their privacy policies, and (b) a reasonable opportunity to withdraw any previously given consents related to the individual's covered data and a reasonable opportunity to request the deletion of the individual's covered data.

14) To ensure the data security and integrity of covered data.

15) With respect to covered data previously collected in accordance with the rules; a service provider acting at the direction of a government entity; or a service provided to a government entity by a covered entity, and only insofar as authorized by statute, to prevent, detect, protect against, or respond to a public safety incident, including trespass, natural disaster, or national security incident. This paragraph does not permit, however, the transfer of covered data for payment or other valuable consideration to a government entity.

16) With respect to covered data collected in accordance with the rules, notwithstanding this exception, to process such data as necessary to provide first-party advertising or marketing of products or services provided by the covered entity for individuals who are

not covered minors, *only if the covered entity provides each affected individual with a reasonable opportunity to withdraw consent for such advertising or marketing*.

E. Require Companies to Disclose Their Data Practices to the FTC and to the Public, and to Submit to Regular Audits.

RDR has extensive experience defining and evaluating standards for disclosing data practices, including those associated with online advertising.[147] Despite these standards constituting a floor rather than a ceiling, few companies that we evaluate meet these expectations.[148] With this in mind, RDR recommends that the Commission establish the following obligations for companies:

- Disclose to users and to the FTC what user information they collect, share, and infer; for what permissible purpose; and for what length of time the information is retained.[149]
- Disclose to users what information they collect from and share with third parties, including information about these third parties, and for what permissible purpose the information is shared or collected.[150]
- Allow users to obtain all of their user information (collected and inferred) held by the company, in a structured data format.[151]
- Delete all user information within a reasonable timeframe after it is no longer needed for its intended permissible purpose, after a user terminates their account, or at the user's request (unless otherwise required by law).
- Submit to regular, independent audits of their data-related practices, including the accuracy of the disclosures above, and provide the results of these audits to the Commission. The Commission should specify the frequency and scope of such audits, taking into consideration company size, industry, and track record of violations related to data processing.

Finally, the Commission should conduct, or commission a reputable, experienced third-party to conduct, a human rights impact assessment (HRIA) of its proposed rulemaking. This HRIA should consider potential unintended effects of its rule-making on populations outside the United States, as determined through consultation with international civil society groups and other experts on international human rights.

---

[147] *See, e.g.*, Ranking Digital Rights, "2020 Indicators," F3(b), F3(c), F4(c) (2020), https://rankingdigitalrights.org/2020-indicators.
[148] *See* Ranking Digital Rights, "The 2022 Big Tech Scorecard, Data Explorer: Targeted Advertising" (2022), https://rankingdigitalrights.org/index2022/explore (showing that no company received more than 47% in targeted advertising-related standards).
[149] *See* Ranking Digital Rights, "2020 Indicators," P3(a), P3(b), P5, P6 (2020), https://rankingdigitalrights.org/2020-indicators.
[150] *See* Ranking Digital Rights, "2020 Indicators," P4, P9 (2020), https://rankingdigitalrights.org/2020-indicators.
[151] *See* Ranking Digital Rights, "2020 Indicators," P7, P8 (2020), https://rankingdigitalrights.org/2020-indicators.

Thank you for your consideration.

Jessica Dheere
Director
Ranking Digital Rights

Nathalie Maréchal, PhD
Policy Director
Ranking Digital Rights

Alex Rochefort
Policy Fellow
Ranking Digital Rights

policy@rankingdigitalrights.org