Comments to the Federal Trade Commission from
Consumer Federation of America and Consumer Action
16 CFR Part 464
Trade Regulation Rule on Commercial Surveillance and Data Security
November 21, 2022

Consumer Federation of America (CFA) and Consumer Action appreciate the opportunity to comment on the Advance Notice of Rulemaking on Commercial Surveillance and Data Security[1] recently issued by the Federal Trade Commission (FTC). CFA, an association of nonprofit consumer organizations and state and local government consumer agencies across the United States, was created in 1968 to advance consumers' interests through research, education, and advocacy. CFA has long worked on issues related to data privacy and security. Consumer Action has been a champion of underrepresented consumers since 1971. A national, nonprofit 501(c)3 organization, Consumer Action focuses on financial education that empowers low to moderate income and limited-English-speaking consumers to financially prosper. It also advocates for consumers in the media and before lawmakers and regulators to advance consumer rights and promote industry-wide change particularly in the fields of consumer protection, credit, banking, housing, privacy, insurance, and telecommunications.

In these comments, CFA and Consumer Action will highlight three specific concerns about "surveillance advertising" and make recommendations for how to address them. CFA has also joined with other groups in comments[2] specifically focusing on children's privacy and strongly supports the broader comments in this proceeding submitted by the Electronic Information Center (EPIC).[3]

Executive Summary

First, the FTC should *prohibit* surveillance advertising, in which individual consumers are shown advertisements based on inferences about their interests, demographics, and other characteristics drawn from tracking their activities over time and space, because it is inherently unfair and deceptive. This practice uses invisible and invasive techniques to manipulate consumers and rob them of real choice in the marketplace. Furthermore, the benefits of surveillance advertising do not outweigh the harms, and relevant ads

[1] Federal Register: Trade Regulation Rule on Commercial Surveillance and Data Security The deadline for comments has been extended to November 21, 2022.

[2] CFA's and Consumer Action's joint comments are at https://consumerfed.org/testimonial/comments-to-the-federal-trade-commission-on-anpr-for-commercial-surveillance-and-security-from-cfa-and-consumer-action/. The child-focused comments which CFA signed onto are also at that link.

[3] EPIC's comments, as well as these comments and those of many other organizations with which we work on privacy, can be found at https://epic.org/ftc-rulemaking-on-commercial-surveillance-data-security/.

can be delivered to consumers in a much less privacy-intrusive manner through contextual advertising.

Second, it is crucial to set rules for data minimization to protect consumers from excessive collection, use, and sale of their data (including sharing their data in exchange for monetary or other forms of valuable consideration). The absence of such protection can result in a range of harms. The FTC should limit the collection, use and sale of data that can be linked to individual consumers to what is necessary to provide them with the products or services they have requested and for other specific permissible purposes.

Third, while notice about surveillance advertising can be useful to consumers and others, the FTC should not over-rely on notice to address the concerns this practice raises. Even if notices about companies' data practices are simplified and standardized, as we believe they should be, not all consumers will read them, and those who do may find it difficult to fully understand the potential impact of these practices. Furthermore, consent to data practices ("choice"), which is usually coupled with notice, can be illusory if consumers *must* agree in order to obtain the information, goods or services they want. Even if notices about data practices are improved and "dark patterns" to manipulate consumers' choices are prohibited, there will always be asymmetries in the balance of knowledge and power between commercial entities and consumers. In the case of surveillance advertising, which by its very nature is not obvious to consumers, notice and consent cannot substitute for limitations and requirements that protect them from unfair and deceptive acts or practices in the collection, use and sale/sharing of their personal information.

In these comments, we will refer to some of the questions that the FTC has posed.

Surveillance advertising should be prohibited.

In January 2022 CFA submitted comments[4] to the FTC in support of a petition[5] by Accountable Tech to prohibit surveillance advertising. CFA noted that the "petition is in line with the recent White House Executive Order that called on federal agencies to combat monopolies and eliminate anticompetitive practices, including those wielded by dominant digital platforms, and specifically encouraged the FTC to use its rulemaking authority to address unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy.[6]

[4] *See* https://consumerfed.org/wp-content/uploads/2022/01/CFA-Supports-Petition-to-Ban-Surveillance-Advertising-Letter-1-26-22.pdf.
[5] *See* https://www.ftc.gov/system/files/attachments/other-applications-petitions-requests/r207005_-_petition_for_rule_to_prohibit_surveillance_advertising_0.pdf.
[6] *See* Promoting Competition in the American Economy, A Presidential Document by the Executive Office of the President, E.O. 14036 of Jul 9, 2021, 86 FR 36987, https://www.federalregister.gov/documents/2021/07/14/2021-15069/promoting-competition-in-the-american-economy.

CFA's comments in that proceeding were informed by its 2021 research on surveillance advertising. Based on that research, CFA produced a series of factsheets[7] that explain what surveillance advertising is, how the tracking that facilitates it works, whether it is good for consumers or the ad tech industry, whether it benefits small business, how it can lead to discrimination, and whether contextual advertising is a better alternative. CFA also created a diagram of the surveillance advertising ecosystem and an infographic. These materials are intended to help policy makers, enforcement agencies, consumer organizations, the media, businesses, and consumers understand surveillance advertising and the concerns it raises.

Surveillance advertising has become a prevalent practice (questions 1, 2 and 3).

According to a survey commissioned by the Interactive Advertising Bureau (IAB), in the United States digital advertising grew tremendously in 2021, and revenues from programmatic advertising, which uses historical traffic data and online targeting methods to display ads to people who are the most likely to want to see them, increased by 39 percent from 2020 to 2021. The study also showed that programmatic advertising increased its share of overall non-search ad revenue to 89.2% (from 88.0% in 2020).[8] It is predicted that in 2022, over 90% of all digital display ad dollars will transact programmatically.[9]

The harms that can arise from surveillance advertising can be substantial and difficult to avoid (questions 4, 5, and 6).

While Accountable Tech's petition to the FTC centered on the anti-competitive nature of surveillance advertising (a concern that CFA shares), CFA's comments noted that this practice is also inherently unfair and deceptive because it "uses invisible and invasive techniques to manipulate consumers and rob them of real choice in the marketplace."[10]

Tracking, profiling, and selling/sharing consumers' data for surveillance advertising often involve entities with which they have no direct relationship (ad tech companies). Since these practices are neither visible to nor expected, consumers are not well-positioned to avoid the harm that may result.

In some circumstances the connection between compilations of their personal data and harm may be obvious to consumers – for instance, when they have been notified of a data breach and subsequently discover that someone is impersonating them using the compromised information to take over their existing accounts or open new ones.[11]

---

[7] *See* https://consumerfed.org/surveillance-advertising-factsheets/.
[8] IAB and PWC, "IAB Internet Advertising Revenue Report: Full Year 2021" (April 2022), https://www.iab.com/video/internet-advertising-revenue-report-full-year-2021-webinar/.
[9] Meagan Yuen, "Programmatic Digital Display Advertising in 2022: Ad spend, formats, and forecast" (May 23, 2022), Insider Intelligence, https://www.insiderintelligence.com/insights/programmatic-digital-display-ad-spending/.
[10] *See* CFA-Supports-Petition-to-Ban-Surveillance-Advertising-Letter-1-26-22.pdf.
[11] Every state in the U.S. has a law requiring individuals whose data has been subject to a breach to be notified.

It is much harder, however, for consumers to be cognizant of harms that may arise from surveillance advertising and avoid them. Most consumers are unaware of the data collection for this purpose and of the profiling that is integral to it. As a 2020 study[12] by Consumer Reports, which traced the evolution of consumers' awareness of and attitudes about online tracking over more than two decades, showed (italics added):

> *"Over time, there has been greater awareness of tracking as a result of consumers' increased experience on the web, personal experiences with corporate tracking and tailored ads, news moments like Cambridge Analytica, and consumer education efforts. Yet, awareness that you are being tracked has not on its own translated into better consumer control over their data. In the current environment, consumers know they are being tracked, but they are largely unaware of how this tracking is done, unable to control such data collection, and may even be resigned or complacent to it."*

Consumer Reports concluded that:

> *"For the majority of the web's existence, the onus to protect and secure private data has largely fallen directly on the consumer, whose data is being collected and used to undermine their autonomy by predicting their behavior, providing them with biased service and pricing, and exploiting their trust to achieve political gains. It is useful to study what consumers know and understand about tracking and tracking technology to reflect on how rampant data collection has led to the current system. However, the initial findings of this research show that awareness of tracking and the techniques by which one is tracked do not on their own empower consumers to better control their data."*

Surveillance advertising can be detrimental to consumers in many ways. For instance, the profiling involved may result in ads not being delivered to consumers for employment, housing, credit, and other economic opportunities:

- ProPublica reported in 2017[13] that employment ads on Facebook from multiple companies were targeted to certain age groups, excluding older workers.
- ProPublica reported in 2018[14] that employment ads from 15 different companies were targeted specifically at either men or women, often along gender-stereotypical lines.

[12] Katie McInnis, "The Evolution of Consumer Attitudes Towards Online Tracking – 1995-2019" (May 2020), Consumer Reports, https://digital-lab.consumerreports.org/wp-content/uploads/2021/02/The-Evolution-of-Consumer-Attitudes-Toward-Online-Tracking_5.20.20_FINAL.pdf.

[13] Julia Angwin, ProPublica, Noam Scheiber, The New York Times, and Ariana Tobin, ProPublica, "Dozens of Companies Are Using Facebook to Exclude Older Workers From Job Ads," ProPublica (December 20, 2017), https://www.propublica.org/article/facebook-ads-age-discrimination-targeting.

[14] Ariana Tobin and Jeremy B. Merrill, "Facebook is Letting Job Advertisers Target Only Men," ProPublica (September 18, 2018), https://www.propublica.org/article/facebook-is-letting-job-advertisers-target-only-men.

- A 2020 study from Carnegie Mellon[15] found discrimination in ads for housing, employment and credit served to non-binary people.

While discrimination in housing, employment, and credit is very concerning, the targeting enabled by surveillance advertising inherently allows advertisers to unfairly discriminate across all types of ads, for any type of products or services. This limits choices available to certain groups of people.

This user tracking and profiling can also be used for price discrimination. For example:

- The Wall Street Journal reported[16] that Staples changed the price shown to users based on their location and distance from rival stores. The article also identified several other companies that adjusted prices depending on a user's location and/or browsing history.
- ProPublica reported in 2015[17] that The Princeton Review charged higher prices for SAT test prep to consumers in ZIP codes with higher percentages of Asian Americans.
- Businesses can also use "price steering" to manipulate user spending based on tracking and profiling.

Price steering attempts to nudge users towards specific options depending on their characteristics. For example:

- Travel website Orbitz sorted search results[18] to show Mac users more expensive hotel rooms than users with other platforms.
- In 2014 researchers at Northeastern University[19] found that 9 out of the 16 ecommerce websites they studied engaged in some sort of price steering or price personalization.

Harms such as these can have substantial impacts on individual consumers and groups of consumers with similar profiles. Since surveillance advertising inherently allows ad targeting based on individuals' personal characteristics, an advertiser can simply decide not to show an ad to certain people.

Even if it is prohibited from using an individual's status in a protected group directly, an

[15] Sara Kingsley, Clara Wang, Alexandra Mikhalenko, Proteeti Sinha, and Chinmay Kulkarni, Carnegie Mellon University, "Auditing Digital Platforms for Discrimination in Economic Opportunity Advertising," (June 2020), https://arxiv.org/ftp/arxiv/papers/2008/2008.09656.pdf.
[16] Jennifer Valentino-DeVries, Jeremy Singer-Vine and Ashkan Soltani, "Websites Vary Prices, Deals Based on Users' Information, The Wall Street Journal (December 24, 2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.
[17] Julia Angwin, Surya Mattu and Jeff Larson, "The Tiger Mom Tax: Asians Are Nearly Twice as Likely to Get a Higher Price from Princeton Review," ProPublica (September 1, 2015), https://www.propublica.org/article/asians-nearly-twice-as-likely-to-get-higher-price-from-princeton-review.
[18] Dana Mattioli, "On Orbitz, Mac Users Steered to Pricier Hotels," The Wall Street Journal (Updated August 23, 2012), https://www.wsj.com/articles/SB10001424052702304458604577488822667325882.
[19] Aniko Hannak, Gary Soeller, David Lazer, Alan Mislove, and Christo Wilson, "Measuring Price Discrimination and Steering on E-Commerce Web Sites," Northeastern University (2014), https://www.ccs.neu.edu/home/cbw/static/pdf/imc151-hannak.pdf#_ga=2.256736264.267237502.1623697468-1938894042.1621527555.

advertiser can use a proxy such as location to exclude protected groups, such as minorities. For instance, an advertiser could use location as a proxy and exclude people in an area in which a particular race or ethnicity is predominant.

The automated processes that facilitate surveillance advertising can lead to discrimination even when ads are targeted fairly. An academic study[20] found that ad delivery is not only based on individuals' personal characteristics; how people respond to advertisements and the amount of money businesses want to spend on advertising also play significant roles in determining who sees what ad.

Some ad tech companies track how different ads perform with different people. If the data show that certain individuals interact with a particular ad more than others, people like them are more likely to be served that ad in the future, to the exclusion of others in that potential audience. Furthermore, since ad delivery operates on an auction system in which businesses bid for ad targets, those that are willing to pay the most will have their ads shown to the most "valuable" individuals, while those who spend less will end up with a less desirable audience for their ads. These practices can skew ad delivery in a way that results in discrimination against certain people, even if that was not the intent.

Other harms that can arise from surveillance advertising and have substantial impacts on consumers include using their profiles to target them for junk food, predatory loans and other dubious products and services, or to deliver misinformation to them for political purposes. As Consumer Reports and EPIC noted in their January 2022 report, *How the FTC Can Mandate Data Minimization through a Section 5 Unfairness Rulemaking*,[21] rather than focusing entirely on specific injuries tied to the collection and use of consumers' data the FTC should recognize that unwanted observation, through excessive data collection and use, is harmful in and of itself. As the FTC knows, personal data can be stolen or used in ways that are inappropriate or unwanted.

If, despite the surreptitious nature of surveillance advertising, consumers are aware of it and wish to avoid harm that may result from it, doing so can be difficult. They can clear cookies on their computers, but not all tracking involves cookies. Ad blockers allow consumers to stop seeing some ads and thus stop some tracking by default, but not all. Some websites and apps offer the ability to opt out of surveillance advertising, but this does not necessarily stop them

[20] Muhammad Ali, Northeastern University, Piotr Sapiezynksi, Northeastern University, Miranda Bogen, Upturn, Aleksandra Korlova, University of Southern California, Alan Mislove, Northeastern University, and Aaron Rieke, Upturn, *Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes*, Proceedings of the ACM on Human-Computer Interaction, Vol. 3, No. CSCW, Article 199 (November 2019), https://dl.acm.org/doi/pdf/10.1145/3359301.

[21] Consumer Reports and the Electronic Privacy Information Center, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (January 26, 2022), https://advocacy.consumerreports.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf, page 6.

from collecting consumers' data. Furthermore, having to opt out of each tracker one-by-one is extremely burdensome for consumers.

There are third-party programs that can help consumers limit surveillance advertising, such as the Digital Advertising Alliance's "Your AdChoices" program,[22] but not all companies participate. Consumers can use Internet browsers with global privacy controls (GPC) to send signals communicating that they do not want their data to be sold or shared, but again, that says nothing about data collection, and the signals may be ignored absent a legal requirement to honor them.

Furthermore, GPC signals have no effect on data collected about consumers offline. License plate readers can track consumers' locations without their knowledge or ability to shield themselves. Consumers also have no control over the use of GPS in vehicles they hire to transport them, such as Ubers. Consumers can turn the location feature off on their mobile devices, but that can interfere with their ability to find their way. Consumers can try to limit the data they provide to companies, but that may also limit the information, products, or services they can obtain. Moreover, consumers have limited control over data about them in public records. It is difficult for consumers to completely avoid the collection of their data for surveillance advertising since their personal information can be obtained from multiple sources.

The harms that can result from surveillance advertising are not outweighed by the benefits (questions 41, 42 and 43).

The argument in favor of surveillance advertising is that consumers appreciate seeing advertisements for products and services in which they are interested. The majority, however, do not want targeted ads when the trade-off is having their personal data collected. A 2021 survey[23] commissioned by Accountable Tech found that 81 percent of Americans would rather keep their personal data private even if it means seeing less relevant ads. Furthermore, a 2019 survey[24] by Pew Research Center found that 79 percent of Americans are concerned about how their data is collected and used by companies, and 81 percent feel that the potential risks of this data collection outweigh the benefits.

Claims that surveillance advertising benefits businesses are also overblown. Publishers – the businesses that operate the websites and apps where the ads appear – do not see revenue

[22] *See*, for example, *YourAdChoices Give You Control*, Digital Advertising Alliance, https://youradchoices.com/.
[23] *See* survey conducted by Greenberg Quinlan Rosner for Accountable Tech (January 28-31, 2012) https://accountabletech.org/wp-content/uploads/Accountable-Tech-Frequency-Questionnaire.pdf, page 4.
[24] 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/.

increase by much, if at all, by hosting targeted ads over non-targeted ones. A 2019 study[25] found that publishers only see a 4 percent increase in revenue from targeted ads over non-targeted ones, or $0.00008 per ad.

Both the New York Times[26] and Dutch public broadcasting company NOP[27] have seen ad revenues increase after they stopped accepting surveillance advertising. Furthermore, surveillance advertising is not as efficient at matching businesses with consumers as some claim.[28] Another 2019 study[29] found that demographics and interest categories used to target ads are often inaccurate across leading data brokers, resulting in low gains for targeted ads over random ad placement.

Contextual advertising is a viable alternative for consumers and businesses (question 41).

There is an effective alternative to deliver relevant ads to consumers – contextual advertising, which is based on characteristics of the *content a consumer is currently browsing* – the subject matter of only that webpage or app. Contextual advertising in its pure form does not take the consumer's characteristics into account or depend on that person's past behavior.[30] Furthermore, as a study[31] in 2020 documented, contextual ads can be more cost-effective for businesses than surveillance advertising.

It is important to note that due to growing concerns about third-party tracking and targeting, the surveillance advertising industry is evolving. Increasingly, first party commercial

[25] Veronica Marotta, Carlson School of Management, University of Minnesota; Vibhanshu Abhishek, Paul Merage School of Business, University California Irvine; and Alessandro Acquisti, Heinz College, Carnegie Mellon University, *Online Tracking and Publishers' Revenues: An Empirical Analysis* (Preliminary Draft, May 2019), https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.

[26] Jessica Davies, "After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue," DIGIDAY (January 16, 2019), https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/.

[27] Natasha Lomas, "Data from Dutch public broadcaster shows the value of ditching creepy ads," Tech Crunch (July 24, 2020), https://techcrunch.com/2020/07/24/data-from-dutch-public-broadcaster-shows-the-value-of-ditching-creepy-ads/.

[28] *See* CFA's *Factsheet: Surveillance Advertising: Does it Benefit Small Business? (*August 26, 2021), https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-small-business/.
[29] Nico Neumann, Catherine E. Tucker, Timothy Whitfield, *Frontiers: How Effective Is Third-Party Consumer Profiling? Evidence from Field Studies,* INFORMS (2019), https://doi.org/10.1287/mksc.2019.118.

[30] See CFA's fact sheet, "*Surveillance Advertising: Is Contextual Advertising a Better Alternative?"* at https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-contextual-is-good-alternative/.
[31] "Landmark Study Proves the Effectiveness of Contextual over Behavioral Targeting," GumGum (2020), https://gumgum.com/blog/landmark-study-proves-the-effectiveness-of-contextual-over-behavioral-targeting.

entities are selling data about their customers to advertisers, and even becoming ad tech companies themselves.[32]

Recommendation 1: The FTC should *prohibit* surveillance advertising because it is inherently unfair and deceptive.

Setting rules for data minimization is crucial to protect consumers from excessive collection, use, sale and sharing of their data.

Data minimization is an essential element of privacy protection (question 43).

There are many definitions of data minimization. For instance, in the European General Data Protection Regulation (GDPR) one of the core principles for processing personal data is that the data must be "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')".[33]

According to the privacy guidelines[34] issued by the Organization for Economic Cooperation and Development "(t)here should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject." This Collection Limitation Principle is meant to be complementary to the other principles in the document, which is intended to be read in its entirety.

A 2021 article in the International Association of Privacy Professionals' newsletter describes the history of the FIPPS (fair information practice principles) around the world, including collection limitations.[35] A recent report by the nonprofit consumer rights organization Access Now describes data minimization as a human rights issue and says, "the simplest and most useful definition is that any organization (whether private company, public entity, or government body) collecting data should collect only the data necessary to provide their product or service, and nothing more."[36]

Why is this principle important for consumer protection? As Access Now puts it, "Expansive data collection has caused significant harm, and risk of harm, for people. These

---

[32] *See* R.J. Cross, "The new data brokers: retailers, rewards apps & streaming services are selling your data," US PIRG (August 2022), https://pirg.org/articles/the-new-data-brokers-retailers-rewards-apps-streaming-services-are-selling-your-data/.

[33] *See* Regulation (EU) 2016/679 of the European Parliament and of the Council, Chapter II, Principles, Article 5 (April 27, 2016), https://gdpr-info.eu/art-5-gdpr/.

[34] *See Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,* Part II, Basic Principles of National Application, 7. (October 7, 2013), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

[35] *See* Cheryl Saniuk-Heinig, CIPP/E, CIPP, "50 years and still kicking: An examination of FIPPs in modern regulation" (May 25, 2021), https://iapp.org/news/a/50-years-and-still-kicking-an-examination-of-fipps-in-modern-regulation/.

[36] Eric Null et al, Access Now, *Data Minimization: Key to Protecting Privacy and Reducing Harm* (May 2021), https://www.accessnow.org/cms/assets/uploads/2021/05/Data-Minimization-Report.pdf.

harms range from the more obvious identity theft and physical harms to less obvious examples, such as relationship harms (due to loss of confidentiality), emotional or reputational harms (due to private information becoming public), or chilling effects on speech or activity (due to a loss of trust in government or other organizations)."[37]

Recommendation 2: In accordance with the data minimization principle, The FTC should limit the collection, use and sale/sharing of data that can be linked to individual consumers to what is necessary to provide them with the products or services they have requested and for other specific permissible purposes.

Notice and consent are not enough.

Notice and consent cannot substitute for limitations and requirements that protect consumers from unfair and deceptive acts or practices in the collection, use and sale/sharing of their personal information **(question 49).**

While there is no comprehensive privacy protection law at the national level in the United States, individual states have begun to act over the past several years. The first was California, which enacted a general privacy statute in 2018.[38] Among other things, the California Consumer Privacy Act (CCPA) entitles individuals to know what personal information companies have collected about them, to ask for the information not to be sold, and to request that their data be deleted (with some exceptions). The CCPA took effect in January 2020 and voters approved a ballot measure last year to strengthen it.

Yet while Californians strongly support the CCPA, a survey that CFA and Consumer Action commissioned in December 2021 showed that large percentages of Internet users in that state had not exercised the rights described above, and the most common reason was that they were unaware of them.[39] (While the survey focused on California Internet users' knowledge and experiences, the CCPA applies to companies' data practices offline as well.)

Black and Hispanic Californians and those at the lower ends of the income and educational scales were especially unaware of these rights. This was notwithstanding the fact that companies offering their products or services to consumers in California must provide information to them about their privacy practices and their rights on their websites, in their stores, on the phone and via the mail. The survey also asked if businesses should be required to obtain individuals' permission to collect, use, or share their personal information for any purpose other than to provide them with the product or service they requested – the data minimization principle. Nine out of ten Californians answered "yes."

---

[37] Id, page 7.

[38] *See* information about the California Consumer Privacy Rights Act on the state attorney general's website at https://www.oag.ca.gov/privacy/ccpa.

[39] *See* press release from CFA and Consumer Action, "Survey Shows Californians Are Still Unaware of Privacy Rights" (January 11, 2022), available at https://consumerfed.org/press_release/survey-shows-californians-are-still-unaware-of-privacy-rights/.

If consumers must take affirmative action to exercise their privacy rights, they cannot do so if they are unaware of those rights and how to assert them. Complicating matters for consumers, companies' privacy policies can be difficult to understand. While many organizations, businesses, and government agencies have worked to make privacy policies easier for consumers to comprehend and to make mechanisms for exercising their choices easier, the fact is that it is a heavy burden for consumers to protect their personal data from unwanted data collection, sharing, and use.

In a 2008 paper, Aleecia M. McDonald and Lorrie Faith Cranor at Carnegie Mellon University estimated that reading privacy policies carried costs in time of 201 hours (about 1 week 1 and a half days) a year, worth about $3,534 annually per American Internet user. They also posited that nationally, if Americans were to read online privacy policies word-for-word, the value of time lost would be $781 billion (about $2,400 per person in the US) annually.[40]

In 2011, Ms. Cranor and colleagues released the results of a 45-participant laboratory study investigating the usability of tools to limit online behavioral advertising. They found "serious usability flaws" in all nine blocking tools participants tested.[41]

Is it realistic to place the burden on consumers to protect themselves from unwanted surveillance advertising? Our answer is "no."

A seminal 2014 paper[42] by Chris Jay Hoofnagle and Jennifer Urban at the University of California, Berkely School of Law explained that:

- "Under the still-dominant U.S. 'notice and choice' approach to consumer information privacy, the rational consumer is expected to negotiate for privacy protection by reading privacy policies and selecting services consistent with her preferences."
- This is difficult, however, because as the authors note, "empirical research supports and goes beyond more general experimental work to reveal that many consumers negotiate privacy preferences based on fundamental misunderstandings about business practices, privacy protections, and restrictions upon the use of data, and that these misunderstandings may lead them to expect more protection than actually exists."

The authors concluded that society should make decisions about information flows and

---

[40] Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies,* I/S: A JOURNAL OF LAW AND POLICY (2008), Vol. 4:3 pages 543-567, available at https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf.

[41] Cranor et al," Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising," (October 31, 2011, revised May 10, 2012), JTHTLv10i2_Cranor.PDF.

[42] Chris Jay Hoofnagle and Jennifer M. Urban, "Alan Westin's Privacy Homo Economicus" (May 19, 2014), 49 Wake Forest Law Review 261 (2014), UC Berkeley Public Law Research Paper No. 2434800, https://ssrn.com/abstract=2434800.

data privacy as machine information processing becomes more sophisticated. Today, that call is even louder as consumers are surreptitiously tracked and judgements are made about what information, products, or services to offer them, at what terms, based on data related to them.

While consumers can easily find information about the relative safety of various models of automobiles to help them make wise purchasing decisions, in many states vehicles that have been deemed unsafe are not allowed to be sold in that condition. The FTC properly protects consumers by providing businesses with guidance and bringing lawsuits to stop unfair acts or practices. The FTC's rulemaking authority is broad, and since 1965 it has promulgated rules to protect consumers from unfair and deceptive practices in a wide range of products and services, from deceptive advertising and labeling of cigarettes in relation to the health hazards of smoking to energy and water use labeling for consumer products.[43] Privacy is addressed in several FTC rules, such as the Telemarketing Sales Rule, the Children's Online Privacy Protection Rule, and the Financial Privacy Rule. It is entirely appropriate for the FTC to initiate this notice of proposed rulemaking concerning commercial surveillance of consumers and to promulgate rules in this regard.

Consumer Reports and EPIC recently produced a paper detailing how the FTC can use its Section 5 unfairness rulemaking authority to mandate data minimization, prohibiting all secondary data uses, with limited exceptions, to ensure that consumers can safely use apps and online services without having to take additional action.[44] We agree.

Recommendation 3: The FTC should use its rulemaking authority to protect consumers from the harms that can arise from the practice of surveillance advertising.

Conclusion

Surveillance advertising uses data to make inferences about consumers, without their knowledge, to customize the information and offers they will see or receive. This practice goes beyond traditional ad targeting, which is relatively easy for consumers to understand. For instance, consumers who subscribe to cooking magazines are not surprised to see ads in them for cooking-related goods or services. If they are at a cooking-related website or using a cooking app, they may also expect to see such solicitations. They may be surprised, however, if the ads they see are different than those presented to other consumers on the same website or using the same app.

To take matters one step further, consumers may not expect that they will see ads for products or services that are completely unrelated to cooking and are based on inferences based on their personal information, especially from companies with which they are unfamiliar.

[43] *See* FTC rules at https://www.ftc.gov/legal-library/browse/rules.
[44] Consumer Reports and the Electronic Privacy Information Center (EPIC), "How The FTC Can Mandate Data Minimization Through A Section 5 Rulemaking" (January 26, 2022), available at https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.

For example, consumers who have diabetes may have special food-related requirements and prohibitions. Is it appropriate for these consumers to be targeted for diabetes medications on cooking websites or apps based on data that have been collected about them? What if the websites or apps on which they are targeted for diabetes medications have nothing to do with food? What if information about their activities using cooking websites or apps, combined with other data, indicates that they are not following eating recommendations for people with diabetes – is it appropriate for that information to be made available to drug companies or health insurers? To potential employers? To companies that are peddling fake diabetes treatments or cures?

CFA and Consumer Action believe that while providing information in companies' privacy policies about data collection, use and sale/sharing can be helpful to consumers, it is insufficient to protect them from potential harm (including unwanted surveillance advertising). They should not be expected to be data practice experts. In some cases, opting into certain surveillance practices may be an appropriate choice to present to consumers if sufficient information is provided and data restrictions are in place; for instance, in offers to participate in loyalty programs offered by companies with which consumers wish to do business. In situations in which consumers' data are needed to prevent fraud, however, providing an opt in is not necessary if the data collection, use, and sharing are restricted to that purpose. Except for necessary operational purposes such as fraud control, secondary data practices should simply be prohibited.

Our organizations look forward to working with the FTC as these and other issues are considered in the rulemaking process. For questions concerning these comments please contact Susan Grant, a Senior Fellow at CFA, sgrant@consumerfed.org, and Ruth Susswein, Consumer Action's Director of Consumer Protection, ruth.susswein@consumer-action.org.