Surveillance Advertising: What is it?

Surveillance advertising, also known as targeted advertising or behavioral advertising, is the practice of showing individual consumers different advertisements based on inferences about their interests, demographics, and other characteristics drawn from tracking their activities over time and space.

Tracking is done[1] primarily by identifying the internet-connected devices that consumers use to search for information, make purchases, engage with social media, play games, watch videos, and participate in other aspects of our increasingly digital lives. When data from these varied activities are combined, it paints detailed portraits of individuals or households, even without personally identifiable information. However, consumers often provide these personal details to create accounts, make transactions, respond to questionnaires, enter contests, and conduct other digital activities, further enriching their profiles. In addition, data brokers sell information about people from public records and commercial sources, which provides another data source for profilers.

The "ad tech" industry is central to surveillance advertising. Ad tech companies conduct tracking, create profiles of consumers, match consumers with ads based on their profiles, and place those ads where they'll see them. Individual companies in this industry may perform some or all of these tasks. Businesses that want to advertise their products or services to people who fit certain profiles (advertisers) pay ad tech companies to find those consumers and deliver ads specifically to them.

On the other side of the equation are businesses that operate the websites and apps where ads appear (publishers). Ad tech companies lurk on publishers' platforms (usually with their permission, but not always), tracking what consumers do there in order to build profiles. When a consumer visits the platform, ad tech companies broadcast the consumer's profile to advertisers (or to other ad tech companies working for advertisers). An automated auction then takes place in a matter of milliseconds to sell the right to advertise to that person.[2] The publisher makes money when the consumer clicks on the ad. Google and Facebook maintain their own ad tech ecosystems, tracking consumers on their platforms and other sites and apps. Based on the consumers' profiles, Facebook shows them ads on its site on behalf of advertisers; Google does the same thing and also delivers targeted ads to consumers on other publishers' websites.

What Are the Concerns About Surveillance Advertising?

Surveillance advertising can perpetuate discrimination in housing, credit, employment, and other economic opportunities.[3] It also hides personalized pricing from consumers,[4] leaving them unaware that a company has charged them a different amount than others. Surveillance advertising is also sometimes used for promoting unhealthy products,[5] encouraging gambling,[6] and perpetrating fraud.[7] The data that are fed into algorithms to profile consumers may be inaccurate,[8] but even when they are correct, the fact is that surveillance advertising is unfair.

1. Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance, Electronic Frontier Foundation, 2019

2. Targeted Online: An industry broken by design and by default, EDRi, 2021

3. Dozens of Companies Are Using Facebook to Exclude Older Workers From Job Ads, ProPublica, 2017

4. Websites Vary Prices, Deals Based on Users' Information, Wall Street Journal, 2012

5. Consumer Groups File FTC Complaint Against PepsiCo for "Deceptive and Unfair Digital Marketing Practices" Targeting Junk Food to Teens, CDD, 2011

6. How is Technology Innovation Impacting Gambling Addiction?, American Addiction Centers, 2019

7. Apps Installed On Millions Of Android Phones Tracked User Behavior To Execute A Multimillion-Dollar Ad Fraud Scheme, BuzzFeed News, 2018

8. More Than Half Of Age Data In Mobile Exchanges Is Inaccurate, AdExchanger, 2017

Consumer Federation of America
1620 Eye Street, NW, Suite 200 · Washington, DC 20006 · (202) 387-6121 · CFA@ConsumerFed.org
www.ConsumerFed.org

It uses invisible and invasive techniques to manipulate consumers and robs them of real choice in the marketplace. Furthermore, the enormous stores of personal data collected for surveillance advertising put consumers at risk for exposure, identity theft, and more malicious tracking.[9] It can also lead to erosion of their 4th Amendment rights, as government agencies can purchase data that otherwise requires a warrant.[10]

9. Data Brokers and Security, NATO Strategic Communications

10. Federal Agencies Use Cellphone Location Data for Immigration Enforcement, Wall Street Journal, 2020

How Can Consumers Avoid Surveillance Advertising?

It is extremely difficult for people to avoid tracking and profiling.[11] Consumers 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. Consumers can use global privacy controls on their internet browsers to send a signal communicating that they don't want their data to be sold, but that says nothing about data collection.[12] Most importantly, companies can simply ignore these signals unless the law requires companies to honor them.

11. California Consumer Privacy Act: Are People Protected?, Consumer Reports, 2020

12. globalprivacycontrol.org, 2021

How Does Surveillance Advertising Affect Small Business?

Facebook touts surveillance advertising as vital for small businesses to connect with consumers efficiently.[13] It's important to remember, though, that Facebook relies on millions of small business advertisers for the bulk of its ad revenue.[14] A 2019 study found that surveillance advertising is not as effective at actually targeting the desired demographic or interest group as previously believed, showing low gains over random ad placement.[15] The idea that small businesses need surveillance advertising to reach consumers is unfounded.

13. Facebook Ad Campaign Promotes Personalized Advertising, Wall Street Journal, 2021

14. Here's how big Facebook's ad business really is, CNN, 2020

15. How Effective Is Third-Party Consumer Profiling? Evidence from Field Studies, INFORMS, 2019

Is There a Good Alternative to Surveillance Advertising?

Yes! Contextual advertising – placing advertisements based on characteristics of the content of a webpage a user is currently browsing – does not require any tracking of individual users. A recent study found contextual advertising to be more cost-effective than targeted advertising.[16] Contextual advertising can also provide more revenue for publishers. Much of the cost of surveillance advertising goes to the various middlemen in the ad tech industry.[17] Since contextual advertising doesn't involve this elaborate infrastructure, more of the ad revenue goes to publishers. Both the New York Times[18] and Dutch public broadcasting company NOP[19] saw revenues increase after they stopped accepting targeted advertising.

16. Landmark Study Proves the Effectiveness of Contextual over Behavioral Targeting, Contextual Insider, 2021

17. Programmatic market a 'mess' with half of money still not reaching publishers, campaign, 2020

18. After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue, Digiday, 2019

19. Data from Dutch public broadcaster shows the value of ditching creepy ads, TechCrunch, 2020

It is important, however, to look closely at what a company is actually doing under the label "contextual advertising." Not all contextual advertising systems are the same, and some so-called contextual advertising systems look more similar to surveillance advertising, taking into account consumer data from online behavior and outside sources.[20]

20. Oracle Audiences, Oracle, 2021

The risks of surveillance advertising outweigh the benefits, and contextual advertising provides a good alternative. Therefore, many organizations in the U.S.[21] and other countries[22] are calling on legislators to ban surveillance advertising.

21. Ban Surveillance Advertising, 2021

22. Ban surveillance-based advertising, Forbrukerradet, 2021