Surveillance Advertising: How Does the Tracking Work?

Ad tech companies that serve targeted advertisements maintain detailed profiles of each consumer. They often contain browsing history, location data, links or advertisements clicked, search history, personal information the consumer has provided, and information purchased from data brokers. Ad tech companies use this data to make inferences about people's demographics, characteristics, and interests. This data collection is ubiquitous and extremely difficult for people to avoid, and it can lead to discrimination, government surveillance, and security issues.

Here are some examples of how ad tech collects consumers' data discretely.

Cookies

Cookies are small text files stored in consumers' browsers when they visit a website.[1] Cookies have legitimate uses outside of tracking and advertising that are necessary for the internet to function as we know it today. For example, a website may use cookies to remember a visitor is logged in when they return. However, ad tech companies can also track people as they traverse the internet by placing cookies on the browser they use. These cookies can be used to store unique user ID numbers which enable trackers to recognize the browser. A cookie can only be read by the party that placed it, so each tracker places its own cookies. A visit to a single website can allow tens or hundreds of companies to set cookies.[2]

Browser Fingerprinting

Browser or device fingerprinting can distinguish one device or browser from another based on certain characteristics, such as the hardware specifications of the device, the fonts that are installed, the browser being used, and the signals the browser sends.[1] When all of these characteristics match, it's a good bet that it's the same device or browser. The Electronic Frontier Foundation found that for a browser chosen at random, only 1 in 286,777 other browsers will share the same fingerprint.[3] Fingerprinting is much harder to detect than cookies because it leaves nothing on the consumer's device, and it's much more difficult for consumers to control since there is nothing to clear or delete. Some browsers, like TOR or Apple's Safari, deploy countermeasures to make fingerprinting more difficult, but it remains a risk.

Mobile Tracking

Cookies and fingerprinting can also be used for tracking when consumers use browsers on mobile devices. However, in apps, trackers must use different methods. Every iOS[4] and Android device has a unique advertising ID built in for the express purpose of surveillance advertising.[1] Consumers can reset this ID, but advertisers can usually still track them using probabilistic matching (described below). Though more difficult to get, trackers also have access to the mobile phone number or the device's hardware ID through some apps on Android (iOS blocks access to these identifiers).[1] Unlike the advertising ID, consumers can't reset these identifiers.

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

2. Web Privacy Census, Technology Science, 2015

3. How Unique Is Your Web Browser?, Electronic Frontier Foundation

4. advertisingIdentifier, Apple Developer

Location Tracking

On a mobile device, many apps gather GPS location data even if they don't actually need it to operate, and then the apps sell this data to ad tech companies.[5] The data are anonymized before it is shared, but it is very easy to "de-anonymize" and link the data to individual consumers.[6] Outside of mobile, an IP address can indicate a consumer's location.[7] IP addresses are based on the network a consumer is connected to, so consumers' IP addresses change as they move around. Though an IP address can't give an exact GPS location, it can identify a consumer's city or even zip code.

Probabilistic Matching

The methods described so far are all device-specific. However, companies know that consumers use multiple devices, and they employ *probabilistic matching* to trace them from one device to the next.[8] By comparing data across different devices – for example, similar search histories or activity on two devices in similar locations – they can determine that the devices likely belong to the same person.

Ever-changing Technology

Because of the wide array of technologies used by trackers and their ever-changing nature, regulation cannot focus on one technology or another. For example, third-party cookies are slowly fading out of use; they have already been blocked by Safari and Firefox, and Chrome plans to block them by 2023.[9] However, as cookies phase out, Google is developing a new tracking method known as FLoC.[10] As another example of new tracking technology, companies are beginning to use cameras in stores to track consumers and the products they may be interested in.[11] Regulating specific tracking technologies only incentivizes trackers to find sneakier ways to profile consumers.

How can consumers avoid being tracked and profiled for surveillance advertising?

It is extremely difficult for people to avoid all of the tracking and profiling that facilitates surveillance advertising.[12] Consumers can clear cookies on their computers, but not all tracking involves cookies, and their use is diminishing. Ad blockers work by rejecting the code that loads ads from running on consumers' browsers and thus stop some tracking by default, but not all; for instance, ad blockers have a harder time preventing fingerprinting, and some tracking code is not associated with ad placement. Furthermore, tracking or ad code can sometimes also be doing something necessary for the webpage to work, and many websites have started requiring users to disable ad blockers in order to access content.[13]

Consumers can use global privacy controls (GPC) on their browsers to send a signal communicating a desire to not have their data sold, but that says nothing about data collection.[14] Moreover, companies can simply ignore these signals unless they are required to honor them. In many cases, consumers must install these tools or turn them on, which can be a complicated and intimidating process.

[5] Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret, New York Times, 2018

[6] How to Track President Trump, New York Times, 2019

[7] IP Geolocation, whatismyipaddress.com

[8] How Ads Follow You from Phone to Desktop to Tablet, MIT Technology Review, 2015

[9] An updated timeline for Privacy Sandbox milestones, Google, 2021

[10] Building a more private web, Google, 2019

[11] Ban Facial Recognition In Stores, 2021

[12] California Consumer Privacy Act: Are People Protected?, Consumer Reports, 2020

[13] getadmiral.com, 2021

[14] globalprivacycontrol.org, 2021

Clicking on options such as “do not sell my data” or “do not track me” on every website a consumer visits is too burdensome. Furthermore, privacy legislation often contains numerous exceptions for certain types of data such as that disclosed on social media, certain types of businesses such as financial institutions and corporate affiliates, and certain uses of data, such as profiling that does not have a “significant legal effect” on the consumer – a determination left up to the business.

The bottom line is that surveillance advertising is unfair. It uses invisible and invasive techniques to manipulate consumers and rob them of real choice in the marketplace. Even if anti-tracking tools come pre-installed on consumers’ devices and are on by default, they will not prevent all tracking and profiling, nor will legal requirements to honor GPC signals guarantee that companies will do so. The risks of surveillance advertising outweigh the benefits, and contextual advertising provides a good alternative. Therefore, many organizations in the U.S. and other countries are calling on legislators to ban surveillance advertising.

See https://consumerfed.org/surveillance-advertising-factsheets/ for more information about surveillance advertising (August 2021).