Online Behavioral Ads Fuel the Surveillance Industry—Here's How

ESPAÑOL

A global spy tool exposed the locations of billions of people to anyone willing to pay. A Catholic group bought location data about gay dating app users in an effort to out gay priests. A location data broker sold lists of people who attended political protests.

What do these privacy violations have in common? They share a source of data that's shockingly pervasive and unregulated: the technology powering nearly every ad you see online.

Each time you see a targeted ad, your personal information is exposed to thousands of advertisers and data brokers through a process called "real-time bidding" (RTB). This process does more than deliver ads—it fuels government surveillance, poses national security risks, and gives data brokers easy access to your online activity. RTB might be the most privacy-invasive surveillance system that you've never heard of.

What is Real-Time Bidding?

RTB is the process used to select the targeted ads shown to you on nearly every website and app you visit. The ads you see are the winners of milliseconds-long auctions that expose your personal information to thousands of companies a day. Here's how it works:

1. The moment you visit a website or app with ad space, it asks a company that runs ad auctions to determine which ads it will display for you. This involves sending information about you and the content you're viewing to the ad auction company.
2. The ad auction company packages all the information they can gather about you into a "bid request" and broadcasts it to thousands of potential advertisers.
3. The bid request may contain personal information like your unique advertising ID, location, IP address, device details, interests, and demographic information. The information in bid requests is called "bidstream data" and can easily be linked to real people.
4. Advertisers use the personal information in each bid request, along with data profiles they've built about you over time, to decide whether to bid on ad space.

5. Advertisers, and their ad buying platforms, can store the personal data in the bid request regardless of whether or not they bid on ad space.

A key vulnerability of real-time bidding is that while only one advertiser wins the auction, all participants receive the data. Indeed, anyone posing as an ad buyer can access a stream of sensitive data about the billions of individuals using websites or apps with targeted ads. That's a big way that RTB puts personal data into the hands of data brokers, who sell it to basically anyone willing to pay. Although some ad auction companies have policies against selling bidstream data, the practice remains widespread.

RTB doesn't just allow companies to harvest your data—it also incentivizes it. Bid requests containing more personal data attract higher bids, so websites and apps are financially motivated to harvest as much of your data as possible. RTB further incentivizes data brokers to track your online activity because advertisers purchase data from data brokers to inform their bidding decisions.

Data brokers don't need any direct relationship with the apps and websites they're collecting bidstream data from. While some data collection methods require web or app developers to install code from a data broker, RTB is facilitated by ad companies that are already plugged into most websites and apps. This allows data brokers to collect data at a staggering scale. Hundreds of billions of RTB bid requests are broadcast every day. For each of those bids, thousands of real or fake ad buying platforms may receive data. As a result, entire businesses have emerged to harvest and sell data from online advertising auctions.

First FTC Action Against Abuse of Real-Time Bidding Data

A recent enforcement action by the Federal Trade Commission (FTC) shows that the dangers of RTB are not hypothetical—data brokers actively rely on RTB to collect and sell sensitive information. The FTC found that data broker Mobilewalla was collecting personal data—including precise location information—from RTB auctions without placing ads.

Mobilewalla collected data on over a billion people, with an estimated 60% sourced directly from RTB auctions. The company then sold this data for a range of invasive purposes, including tracking union organizers, tracking people at Black Lives Matter protests, and compiling home addresses of healthcare employees for recruitment by competing employers. It also categorized people into custom groups for advertisers, such as "pregnant women," "Hispanic churchgoers," and "members of the LGBTQ+ community."

The FTC concluded that Mobilewalla's practice of collecting personal data from RTB auctions where they didn't place ads violated the FTC Act's prohibition of unfair conduct. The FTC's proposed settlement order bans Mobilewalla from collecting consumer data from RTB auctions for any purposes other than participating in those auctions. This action marks the first time the FTC has targeted the abuse of bidstream data. While we celebrate this significant milestone, the dangers of RTB go far beyond one data broker.

Real-Time Bidding Enables Mass Surveillance

RTB is regularly exploited for government surveillance. As early as 2017, researchers demonstrated that $1,000 worth of ad targeting data could be used to track an individuals'

locations and glean sensitive information like their religion and sexual orientation. Since then, data brokers have been caught selling bidstream data to government intelligence agencies. For example, the data broker Near Intelligence collected data about more than a billion devices from RTB auctions and sold it to the U.S. Defense Department. Mobilewalla sold bidstream data to another data broker, Gravy Analytics, whose subsidiary, Venntell, likewise has sold location data to the FBI, ICE, CBP, and other government agencies.

In addition to buying raw bidstream data, governments buy surveillance tools that rely on the same advertising auctions. The surveillance company Rayzone posed as an advertiser to acquire bidstream data, which it repurposed into tracking tools sold to governments around the world. Rayzone's tools could identify phones that had been in specific locations and link them to people's names, addresses, and browsing histories. Patternz, another surveillance tool built on bidstream data, was advertised to security agencies worldwide as a way to track people's locations. The CEO of Patternz highlighted the connection between surveillance and advertising technology when he suggested his company could track people through "virtually any app that has ads."

Beyond the privacy harms from RTB-fueled government surveillance, RTB also creates national security risks. Researchers have warned that RTB could allow foreign states and non-state actors to obtain compromising personal data about American defense personnel and political leaders. In fact, Google's ad auctions sent sensitive data to a Russian ad company for months after it was sanctioned by the U.S. Treasury.

The privacy and security dangers of RTB are inherent to its design, and not just a matter of misuse by individual data brokers. The process broadcasts torrents of our personal data to thousands of companies, hundreds of times per day, with no oversight of how this information is ultimately used. This indiscriminate sharing of location data and other personal information is dangerous, regardless of whether the recipients are advertisers or surveillance companies in disguise. Sharing sensitive data with advertisers enables exploitative advertising, such as predatory loan companies targeting people in financial distress. RTB is a surveillance system at its core, presenting corporations and governments with limitless opportunities to use our data against us.

How You Can Protect Yourself

Privacy-invasive ad auctions occur on nearly every website and app, but there are steps you can take to protect yourself:

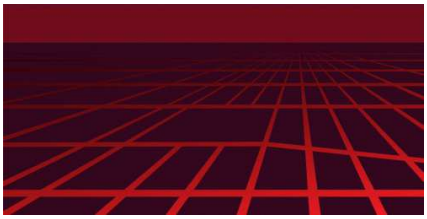
- For apps: Follow EFF's instructions to disable your mobile advertising ID and audit app permissions. These steps will reduce the personal data available to the RTB process and make it harder for data brokers to create detailed profiles about you.
- For websites: Install Privacy Badger, a free browser extension built by EFF to block online trackers. Privacy Badger automatically blocks tracking-enabled advertisements, preventing the RTB process from beginning.

These measures will help protect your privacy, but advertisers are constantly finding new ways to collect and exploit your data. This is just one more reason why individuals shouldn't bear the sole responsibility of defending their data every time they use the internet.

The Real Solution: Ban Online Behavioral Advertising

The best way to prevent online ads from fueling surveillance is to ban online behavioral advertising. This would end the practice of targeting ads based on your online activity, removing the primary incentive for companies to track and share your personal data. It would also prevent your personal data from being broadcast to data brokers through RTB auctions. Ads could still be targeted contextually—based on the content of the page you're currently viewing—without collecting or exposing sensitive information about you. This shift would not only protect individual privacy but also reduce the power of the surveillance industry. Seeing an ad shouldn't mean surrendering your data to thousands of companies you've never heard of. It's time to end online behavioral advertising and the mass surveillance it enables.

RELATED UPDATES



DEEPLINKS BLOG BY LENA COHEN, HUDSON HONGO | MARCH 5, 2026

The Government Uses Targeted Advertising to Track Your Location. Here's What We Need to Do.

The online advertising industry has built a massive surveillance machine, and the government can co-opt it to spy on us.

DEEPLINKS BLOG BY LENA COHEN | JANUARY 29, 2026

Google Settlement May Bring New Privacy Controls for Real-Time Bidding

EFF has long warned about the dangers of the "real-time bidding" (RTB) system powering nearly every ad you see

online. A proposed class-action settlement with Google over their RTB system is a step in the right direction towards giving people more control over their data. Truly curbing the harms of...

DEEPLINKS BLOG BY LENA COHEN | SEPTEMBER 4, 2025

From Libraries to Schools: Why Organizations Should Install Privacy Badger

In an era of pervasive online surveillance, organizations have an important role to play in protecting their communities' privacy. Schools, libraries, and other organizations can make private browsing the norm by deploying Privacy Badger on their computers.

DEEPLINKS BLOG BY LENA COHEN, RORY MIR | JUNE 20, 2025

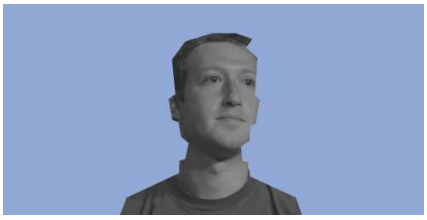
Protect Yourself From Meta's Latest Attack on Privacy

The best way to stop this cycle of invasive tracking techniques and patchwork fixes is to ban online behavioral advertising. This would end the practice of targeting ads based on your online activity, removing the primary incentive for companies to track and share your personal data. We need strong federal...

DEEPLINKS BLOG BY LENA COHEN | MARCH 27, 2025

Online Tracking is Out of Control—Privacy Badger Can Help You Fight Back

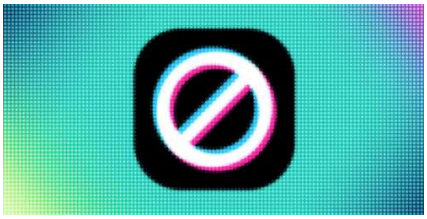
Every time you browse the web, you're being tracked. That's why EFF created Privacy Badger, a free, open source browser extension used by millions to fight corporate surveillance and take back control of their data.



DEEPLINKS BLOG BY LENA COHEN | JANUARY 17, 2025

Mad at Meta? Don't Let Them Collect and Monetize Your Personal Data

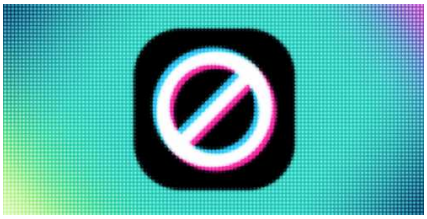
If you're fed up with Meta right now, you're not alone. Meta tracks you across millions of websites and apps and its business model relies on your data. If you want to limit Meta's ability to collect and profit from your personal data, here's what you need to know.



DEEPLINKS BLOG BY DAVID GREENE | JANUARY 17, 2025

EFF Statement on U.S. Supreme Court's Decision to Uphold TikTok Ban

Shutting down a communications platform or forcing its reorganization based on concerns of foreign propaganda and anti-national manipulation is an eminently anti-democratic tactic, one that the US has previously condemned globally.



DEEPLINKS BLOG BY DAVID GREENE | DECEMBER 18, 2024

EFF Statement on U.S. Supreme Court's Decision to Consider TikTok Ban

The TikTok ban itself and the DC Circuit's approval of it should be of great concern even to those who find TikTok undesirable or scary. Shutting down communications platforms or forcing their reorganization based on concerns of foreign propaganda and anti-national manipulation is an eminently anti-democratic tactic, one that the...

DEEPLINKS BLOG BY CHRISTIAN ROMERO | OCTOBER 31, 2024

"Is My Phone Listening To Me?"

Whether you're just starting to question some of the effects of technology in your life or you're the designated tech wizard of your family looking for resources to share, Digital Rights Bytes is here to help answer some common questions that may be bugging you about the devices you use.

DEEPLINKS BLOG BY GUEST AUTHOR, ERICA PORTNOY | OCTOBER 1, 2024

How to Stop Advertisers From Tracking Your Teen Across the Internet

When children turn 13, they age out of the data protections provided by the Children's Online Privacy Protection Act (COPPA). Then, they become targets for data collection from data brokers that collect their information from social media apps, shopping history, location tracking services, and more.