FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Technology Blog

Unpacking Real Time Bidding through FTC's case on Mobilewalla

By: Staff in the Office of Technology & Division of Privacy and Identity Protection | December 3, 2024

The FTC recently announced a new enforcement action in which it alleged that the data broker Mobilewalla collected and retained sensitive location information from consumers—often without their consent—and shared those details with third parties to target advertisements. This data can reveal visits to healthcare facilities, churches, labor unions, military installations, and other sensitive locations. While it is hardly the first time the FTC has taken action against such unfair data collection practices, the Mobilewalla case shines a new spotlight on the collection and use of data through ad exchanges, the invisible intermediaries that auction off digital space to advertisers. The remedies in the case include the agency's first provisions restricting the use of consumer data, including precise location data, that bidders can access as part of that auction process. This includes a ban on collecting or retaining data for any purpose other than participating in those auctions.

The Mobilewalla case demonstrates how different technologies are being used by digital companies to harvest consumer data. The FTC will continue to enforce the law against companies collecting sensitive consumer data—such as a person's location, the names of apps they use, or their unique mobile identifiers—in unfair or deceptive ways, no matter what digital mechanism is used.

Over the past few decades, advertising has evolved from a process commanded by Mad Men-esque boardrooms to one that is almost entirely run by algorithms. Most of the advertisements you see online involve a process called "real-time bidding" (RTB), where publishers—in this case, the websites, apps, or other digital mediums with ad space to sell—auction off their empty ad space on exchange platforms, and advertisers can bid for that placement. To ensure that the best-suited advertiser is reaching the best-suited consumer, exchanges sometimes include granular details like location or personal characteristics about the people downstream who could be the target of an ad.

These broadcasts occur over the milliseconds it takes an ad to populate on a person's screen, making it hard to comprehend exactly how much data gets collected in that instant, and the number of players to which that data gets routed.

The use of real-time bidding presents potential concerns:

1. **Ad auctions incentivize invasive data-sharing.** Publishers and other intermediaries involved with auctions can share a range of details about consumers. There are no hard-and-fast rules governing which specific datapoints get disseminated during a given auction. In fact, buyers have historically pushed publishers to share as much end-user data as possible to get higher valuation for their ad inventory—particularly their location data and cookie cache, which can be used to ascertain a person's browsing history and behavior.

2. **Ad auctions can send sensitive data across geographic borders.** Ad exchanges transact with both publishers and bidders programmatically, which means that data can be sent across geographic borders with little effort. U.S. lawmakers have previously highlighted the potential for exchanges to inadvertently transmit datapoints like consumers' precise location and online behavior to adversarial parties operating overseas, who could potentially exploit that data for surveillance, blackmail, or social engineering campaigns.

3. **Ad auctions are designed to broadcast sensitive data widely and can shelter bad actors who exploit that data.** Though ad auctions might be invisible to consumers, past research has shown that some popular ad exchanges can handle tens of billions of auctions per day. Each auction involves a broadcast of consumer data being sent to potentially dozens of bidders simultaneously, despite only one of those parties—the winning bidder—actually using that data to serve a targeted ad. Experts have previously cautioned that there are few (if any) technical controls ensuring those other parties do not retain that data for use in unintended ways. The complaint against Mobilewalla, for example, alleges that the company was collecting and retaining data gleaned from ad auctions it had lost, despite those same exchanges explicitly prohibiting non-advertising uses of that same consumer data.

As the agency has stated previously, location data is sensitive data, full stop. Location data can reveal where we live, work, and worship, where we seek medical treatment, and even our presence at a protest or political event. Tackling the privacy concerns involved with real-time bidding might be a new frontier, but that will not stop the agency's track record of enforcing the law against companies that collect, use, and share consumers' sensitive data without their consent.

Thank you to the contributors of this post: Shoshana Wodinsky, David Walko, Aaron Alva, Amritha Jayanti, Ben Wiseman, Stephanie T. Nguyen, Sam Levine

Tags: Consumer Protection | Bureau of Consumer Protection | Data security | Technology | Privacy and Security | Office of Technology

More from the Technology Blog

Technology Blog

AI and the Risk of Consumer Harm

Staff in the Office of Technology and the Division of Advertising Practices | January 3, 2025

Technology Blog

Lenses of security: Preventing and mitigating digital security risks through data management, software development, and product design for humans

Staff in the Office of Technology & the Division of Privacy and Identity Protection | December 13, 2024

Technology Blog

Solving the Traveling Salesman Problem? Not quite, but here are more research questions from the Office of Technology

Staff at the Office of Technology | December 4, 2024

Technology Blog

Data Clean Rooms: Separating Fact from Fiction

Staff in the Office of Technology and the Division of Privacy and Identity Protection | November 13, 2024