The ongoing massive data breach in the world of advertising: real time bidding ("RTB").

You likely are, or have been, a target of RTB without your knowledge. The Irish Council for Civil Liberties ("ICCL") found that the typical EU user's data is shared an average of 376 times per day, and the typical US user's data is shared an average of 747 times per day through the RTB practice.

**How does RTB work?**

When a user visits a website and accepts its cookies request, including marketing
cookies, ad brokers (such as Interactive Advertising Bureau ("IAB")) place cookies on
the user's browser to track and collect specific information about the user. This
information includes personal, yet seemingly nondescript, data such as device
identifiers (device type, brand, model, screen size, connection type, operating
system, and CPU speed); IP addresses; zip/postal codes; GPS locations; browsing
history; and search results. The cookies do not collect the more traditionally
considered personal information such as the user's name, email address, address, or
phone number.

Despite the seemingly nondescript nature of the data collected, the information that
can be gleaned is significant and is compiled to create a profile of the user. A user's
profile includes information such as religious belief, sexual orientation, political
affiliation, gender, age, education level, debt, health status, pregnancy status, and
much more.

What's the Purpose of RTB?

Predictive advertising. These user profiles are sold to the highest bidder and are
used to push ads to the user. Specifically, when a user visits another
website containing ads, the ad broker auctions that profile information to the
highest paying advertiser for the right to show its ad to the user.

What's the Harm Caused by RTB?

First, ad brokers are not necessarily only using the data for marketing. The highest
bidders for these profiles can be any third party, including bad actors, watchdog
agencies, governmental agencies, and organizations in nations such as China or
Russia.

In addition, while ad brokers are not collecting certain personally identifiable
information, such as name, email address, address, identification numbers, or phone
number, given enough data points, a person's identity could be generally inferred.
According to the Wall Street Journal, after about two hundred fifty (250) likes on a
social media platform, marketing companies can use technology to understand a
user better than the user's spouse.

Furthermore, even with a user presumably providing consent, there are significant
data breach concerns with RTB:

1. Lack of Knowledgeable Consent

   Though ad brokers are asking consent for marketing from users, they are not
gathering consent to share that data with thousands of their customers. Users
are not informed of how their data will be used and shared, thus unable to
provide affirmative consent.

2. High-velocity, Unsecure Transfer of Data on Massive Scale

   The high-velocity, massive scale transmittance of user data over the internet to
thousands of recipients (with the risk of interception by other parties) is
inherently insecure. Bad actors can intercept the information transmitted over
the internet by ad brokers. Given the volume of data transmitted, the chances of interception increase.

RTB Accountability?

During its investigation, the Belgian Data Protection Authority ("Belgian DPA") found that the transparency and consent framework used by ad brokers involved in RTB does not comply with GDPR principles of transparency, fairness, accountability, and lawfulness of processing. Between the inappropriate consent and insecure data transfer, and given the massive scale of data involved, RTB was deemed "the biggest data breach ever recorded. And it is repeated every day."

The Belgian DPA provided IAB with two (2) months to provide a plan on how to reform the practice with another six (6) months to implement the changes. After which, IAB will face a € 5,000 fine each day it remains out of compliance. Meanwhile, IAB has also incurred a € 250,000 fine for its initial non-compliance.

How Can You Protect Yourself?

While a decision has been issued by the Belgian DPA, threats to users' data continue to be a reality in the vast void of the internet. To protect yourself, we recommend:

- Understanding the data you provide or share access to when browsing websites and using mobile applications.
- Reading the Privacy Policy and Terms of Use to know what rights you are granting for using your data.
- Limiting the permissions granted to a mobile application to only those parts of your phone, tablet, or computer absolutely necessary for the application to function (e.g., does a crossword app need access to GPS, camera, and microphone?)
- Limiting the permissions to "just this once" as opposed to "always."
- Declining consent to advertising or marketing on websites, especially websites you do not trust.
- Limiting the cookies accepted to those cookies absolutely necessary to use a website. Often the "strictly necessary" cookies are enough to use a website.
- Regularly clear your cookies, browsing history, saved search results, and browser cache.

© 2022 Ward and Smith, P.A.. All Rights Reserved.

National Law Review, Volume XII, Number 189

Source URL: https://www.natlawreview.com/article/going-once-going-twice-sold-