Unfair & Deceitful Commercial Surveillance
Submission to the United States Federal Trade Commission

November 2022

Dr Johnny Ryan FRHistS
Senior Fellow, ICCL and Senior Fellow, Open Markets Institute
In this submission

Evincing the FTC’s authority to act ........................................ 3
Prevalent & unavoidable .......................................................... 4
Sensitivity of the data ............................................................... 6
Lack of security ........................................................................ 7
Harms to people’s privacy ........................................................... 9
Harms to the market ................................................................. 10
Who benefits? .......................................................................... 14
Deception .................................................................................. 15
Conclusion .................................................................................. 16

Contact: johnny.ryan@iccl.ie
Evincing the FTC’s authority to act

This submission demonstrates that the Commission can and should act to protect people from commercial surveillance. The hazards of commercial surveillance are real.

- Our submission focusses on Real-Time Bidding (RTB). RTB is the dominant system of online advertising, and provides billions of records for the data broker industry. The practices of RTB illustrate how commercial surveillance operate.

- The practices are unfair. The ubiquity of the RTB system, and the frequency of RTB broadcasts, make it prevalent and unavoidable. The massive volume of data broadcast by RTB, and the sensitivity of the data, expose people to significant injury. It also causes serious harms for consumers who want publishers to be sustainable, and offers no countervailing benefit.

- The false “consent” and disclosure pop-ups for RTB are a deception on an industrial scale. People are asked to consent to these practices, but it is impossible for them to be adequately informed, and their rejection will in any case not be honored. This compliance theatre is not only deception, but nuisance spam, too.

- In addition, commercial surveillance poses a serious national security hazard.
Prevalent & unavoidable

The private things we do and watch online, and where we move in the real world, are collected from a vast online system that operates behind the scenes on virtually every website and app. It is called “Real-Time Bidding” (RTB).

- RTB is the dominant technology of online advertising.¹ Almost every time you load a page on a website, or use an app,² an RTB auction determines what ad will appear in front of you.

- Google is the biggest of several major RTB companies.³ Its system is live on 7.2 million websites⁴ and broadcasts data such as what people are viewing or doing on a website or app and their “hyperlocal”⁵ locations 31 billion times every day in the U.S.

- RTB is prevalent and unavoidable: it tracks and broadcasts what every U.S. internet user does twice per minute that they are online.⁶

- Americans are exposed in this manner 107 trillion times a year by the RTB industry.⁷ This is the biggest data breach ever.


The chart shows the billions of RTB broadcasts about people every day in each State. These figures are lower than the reality: we do not have data for Facebook and Amazon.
Daily number of broadcasts of each person’s data

On average, the RTB system broadcasts what a person in the U.S. is reading and watching, and where they are, 747 times a day. For example, a person in Ohio will have their online activity and location exposed 812 times every day. See data about each State below. These figures are lower than the reality: we do not have data for Facebook and Amazon.

<table>
<thead>
<tr>
<th>State</th>
<th>Daily Broadcasts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Colorado</td>
<td>987</td>
</tr>
<tr>
<td>Michigan</td>
<td>913</td>
</tr>
<tr>
<td>Illinois</td>
<td>912</td>
</tr>
<tr>
<td>North Carolina</td>
<td>911</td>
</tr>
<tr>
<td>Washington</td>
<td>893</td>
</tr>
<tr>
<td>Minnesota</td>
<td>892</td>
</tr>
<tr>
<td>Wisconsin</td>
<td>878</td>
</tr>
<tr>
<td>Florida</td>
<td>870</td>
</tr>
<tr>
<td>Nebraska</td>
<td>868</td>
</tr>
<tr>
<td>Georgia</td>
<td>851</td>
</tr>
<tr>
<td>Missouri</td>
<td>844</td>
</tr>
<tr>
<td>Massachusetts</td>
<td>840</td>
</tr>
<tr>
<td>Oregon</td>
<td>826</td>
</tr>
<tr>
<td>Pennsylvania</td>
<td>821</td>
</tr>
<tr>
<td>Iowa</td>
<td>816</td>
</tr>
<tr>
<td>New York</td>
<td>814</td>
</tr>
<tr>
<td>Maryland</td>
<td>814</td>
</tr>
<tr>
<td>Ohio</td>
<td>812</td>
</tr>
<tr>
<td>Nevada</td>
<td>808</td>
</tr>
<tr>
<td>California</td>
<td>804</td>
</tr>
<tr>
<td>Tennessee</td>
<td>799</td>
</tr>
<tr>
<td>Delaware</td>
<td>797</td>
</tr>
<tr>
<td>Virginia</td>
<td>785</td>
</tr>
<tr>
<td>Arizona</td>
<td>782</td>
</tr>
<tr>
<td>New Hampshire</td>
<td>770</td>
</tr>
<tr>
<td>Kansas</td>
<td>763</td>
</tr>
<tr>
<td>Indiana</td>
<td>753</td>
</tr>
<tr>
<td>Maine</td>
<td>750</td>
</tr>
<tr>
<td>Texas</td>
<td>748</td>
</tr>
<tr>
<td>Connecticut</td>
<td>745</td>
</tr>
<tr>
<td>North Dakota</td>
<td>743</td>
</tr>
<tr>
<td>Utah</td>
<td>730</td>
</tr>
<tr>
<td>Montana</td>
<td>698</td>
</tr>
<tr>
<td>Vermont</td>
<td>684</td>
</tr>
<tr>
<td>New Jersey</td>
<td>677</td>
</tr>
<tr>
<td>Wyoming</td>
<td>671</td>
</tr>
<tr>
<td>South Dakota</td>
<td>670</td>
</tr>
<tr>
<td>Idaho</td>
<td>659</td>
</tr>
<tr>
<td>Arkansas</td>
<td>657</td>
</tr>
<tr>
<td>Rhode Island</td>
<td>651</td>
</tr>
<tr>
<td>Hawaii</td>
<td>649</td>
</tr>
<tr>
<td>Oklahoma</td>
<td>629</td>
</tr>
<tr>
<td>West Virginia</td>
<td>625</td>
</tr>
<tr>
<td>South Carolina</td>
<td>625</td>
</tr>
<tr>
<td>Alabama</td>
<td>616</td>
</tr>
<tr>
<td>Kentucky</td>
<td>598</td>
</tr>
<tr>
<td>Louisiana</td>
<td>556</td>
</tr>
<tr>
<td>Alaska</td>
<td>553</td>
</tr>
<tr>
<td>New Mexico</td>
<td>546</td>
</tr>
<tr>
<td>Mississippi</td>
<td>493</td>
</tr>
<tr>
<td>District of Columbia</td>
<td>486</td>
</tr>
</tbody>
</table>

(D.C. day time commuter adjusted population used)
Sensitivity of the data

- RTB data broadcasts can include what a person is reading or watching or listening to at that moment, and where they are physically - sometimes right up to the person’s GPS coordinates (or “hyperlocal coordinates” in Google’s version of RTB).^10

- RTB data broadcasts can also include the category of content a person is viewing and interested in. For example, a person likely to have suffered sexual violence can be assigned the code IAB7-28, which denotes “Incest/abuse support,” or “AIDS/HIV” (code: IAB 7-3), “Bipolar Disorder” (IAB 7-9), “Infertility” (IAB 7-30), etc. There are hundreds such codes for peoples’ intimate health conditions and religious faith.

- The RTB system broadcasts this sensitive data along with ID codes that identify the specific person concerned. This allows “data broker” companies to accumulate RTB data about every American online: what they have read, watched, listened to, and done, and everywhere they have been.


---

Example of a data broker that uses RTB data: Mobilewalla

Mobilewalla claims to have 4 years of data from 1.6 billion people’s devices. RTB is one of its main sources. Its CEO says RTB data can even show frequency of church attendance:

> “the first thing we must do is to store ad requests over time — to identify regular churchgoers, we must figure out which devices have appeared in churches weekly over a period of six months—this needs at least six months of stored ad requests.”

Mobilewalla processes “tens of terabytes of data a day” to collect people’s GPS coordinates, homes, work locations and what they do on their phones. It categorizes people by ethnicity (for example based on their phone use during Ramadan, or “were observed frequently in mosques”), by income, and other intimate characteristics.
Lack of security

- A single RTB auction to show a single person a single ad can broadcast that person’s intimate secrets to “thousands” of companies, according to industry documentation. One such auction can involve many sub-auctions, each run by a separate RTB “ad exchange”. Google says that 4,698 firms may receive data from its Ad Exchange. Microsoft Xandr says 1,647 firms may receive data from its Ad Exchange. There are many others.

- There is no way to restrict the spread of RTB data about everyone’s physical movements and their online activities after broadcast. This is confirmed by industry technical documentation, UK regulatory investigation, and EU-wide enforcement action. There are commercial reasons to share it widely with business partners, or anyone else who will pay. RTB is a massive, systematic data breach.

- Google and other RTB companies share these data with entities all over the world, including companies in Russia and China. There is no way to know what these firms do with the data. Other RTB companies are equally careless with American’s secrets.

---

**How Real-Time Bidding broadcasts a person’s data**

**Step 1.** A person loads a webpage

**Step 2.** Supply Side Platform (SSP) sends personal data (RTB bid request) to one or more Ad Exchanges

**Step 3.** Ad Exchanges broadcast the personal data (RTB bid request) to many Demand Side Platforms (DSPs)

Legend

- Not observable
- Observable

---

Unfair & Deceitful Commercial Surveillance
NATIONAL SECURITY RISK

- **Google** and other RTB companies broadcast the intimate behavior of Americans to “thousands”\(^{30}\) of companies around the world, including in China\(^ {31}\) and Russia,\(^ {32}\) even including sanctioned companies,\(^ {33}\) without any control over what then happens to that data.\(^ {34}\)

- This exposes sensitive personnel to risk of compromise by foreign adversaries. For example, IAB code 885 marks a person as being in procurement (“purchase intent”) in the “Aerospace and Defense” sector.\(^ {35}\) IAB, the tracking industry trade body, has other codes to attach “online gambling”, “debt”, and “bankruptcy” to that person’s profile, too.

- In April 2021, lawmakers wrote to major RTB firms noting that RTB “bidstream” data “would be a **goldmine for foreign intelligence services** that could exploit it to inform and supercharge hacking, blackmail, and influence campaigns”.\(^ {36}\)

- Congress is considering directing the Director of National Intelligence to **investigate whether intelligence personnel have been tracked by foreign adversaries** using RTB and other advertising technology data.\(^ {37}\)

- U.S. Special Operations Command purchased RTB data in the form of a product called Locate X.\(^ {38}\) However, RTB exposes not only adversaries, but U.S. personnel too: it revealed the **movements of individual US military special operators** in Syria and Kuwait, and at Fort Bragg and Fort Hood.\(^ {39}\)

- The U.S. Cybersecurity & Infrastructure Security Agency recommended all federal agencies to block ads to reduce the “**risk of data collection** by third parties”.\(^ {40}\)
Harms to people’s privacy

In addition to the national security risk that threatens all Americans, commercial surveillance also exposes each American to direct substantial injuries such as predation, discrimination, diminution of their personal autonomy and freedom to act, and unwarranted intrusion by Government.

- The US Department of Homeland Security and other agencies used Mobilewalla RTB data for warrant-less phone tracking.\(^41\)

- Mobilewalla used RTB data to illicitly profile the ethnicity and track the movements of Americans in protests in New York, Los Angeles, Minneapolis and Atlanta. Lawmakers asked the FTC to investigate.\(^42\)

- RTB was implicated in predatory profiling of vulnerable people, such as a suicidal gambling addict.\(^43\)

- ICCL uncovered the sale of RTB data revealing likely survivors of sexual abuse and incest.\(^44\)

- The Norwegian Consumer Council reported that the gay and trans dating app Grindr broadcasting RTB data about users\(^45\). RTB data was subsequently implicated in the outing of a gay Catholic priest through his use of Grindr.\(^46\)

- ICCL discovered in 2019 that Google’s RTB system allows companies to target 1,200 people in Ireland profiled in a “Substance abuse” category, based on a data broker profile built with RTB data. Other health condition profiles from the same data broker available via Google included “Diabetes”, “Chronic Pain”, and “Sleep Disorders”.\(^47\)

- The sale of people’s live RTB location data is now commonplace. Millions of Americans were tracked by the CDC to see if they complied with Covid Lockdowns, using RTB data from Safegraph.\(^48\)

- Many different county sheriffs departments were able to purchase people’s live location and movements from “Fog Data Science”, which gathers data from mobile apps (presumably\(^49\) using RTB). The FTC has been asked to investigate.\(^50\)
Harms to the market

Commercial surveillance harms consumer choice by imperiling publisher sustainability in four ways.

**BOT FRAUD**

- The RTB system is easily tricked by criminals to spend advertisers’ budgets on fraudulent websites, showing ads to “bots” that masquerade as human viewers.

- Even Facebook does not know whether an interaction is by a human or a bot. Facebook removed 3 billion fake accounts in the first half of 2022, and a further 6.5 billion fake accounts in 2021. For context, Facebook claims only 2.9 billion active monthly users.

- Some websites are intended never to be seen by humans. They do nothing but show ads to bots. A study commissioned by US Association of National Advertisers estimated that these websites make up 20% of the Internet.

- All estimates agree that “ad fraud” nets criminals billions of dollars every year.

---

**Chart: Billions of dollars of tracking-based fraud**

Estimates and forecasts of tracking-based fraud in digital advertising.

<table>
<thead>
<tr>
<th>Year</th>
<th>Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>$6.3bn</td>
</tr>
<tr>
<td>2016</td>
<td>$7.2bn to $7.6bn</td>
</tr>
<tr>
<td>2018</td>
<td>$6.5bn</td>
</tr>
<tr>
<td>2020</td>
<td>$32bn</td>
</tr>
<tr>
<td>2022</td>
<td>$100bn</td>
</tr>
<tr>
<td>2024</td>
<td>$50bn to $140bn</td>
</tr>
</tbody>
</table>

Note: ANA estimates are for US market. Juniper, CHEQ, and WFA estimates are global.
BIG TECH THEFT OF DATA FROM PUBLISHERS

- Google and Facebook both collect more data from other companies (including publishers) than they collect from their own user-facing products, according to the UK Competition & Markets Authority.\(^{55}\)

- Leakage of publishers’ audience data fuels Google & Facebook businesses at publishers’ expense. For example, Google’s terms make clear that “Google uses the information shared by [publishers] sites and apps to … personalize content and ads you see on Google … sites and apps”.\(^{56}\)

Google siphoned publisher audience data for itself

Half of Google’s ad revenue once came from helping publishers show ads on publishers’ own properties. But now nearly all (85%) of Google’s ad revenue comes from displaying ads on its own websites and apps, with the benefit of data siphoned from publishers’ websites & apps.
OPAQUE “ADTECH TAX”

- RTB enables tech firms to charge opaque fees, known in the industry as “adtech tax”. In a widely cited experiment, The Guardian bought ads on its own website. It discovered that of every £1 that it spent as an advertiser it received only 30p as the publisher. 70% disappeared into the RTB industry.\(^\text{57}\)

- $35-69bn of the $99bn invested by advertisers in video and display ads in 2021 is likely to have been siphoned off by tech companies, away from publishers.\(^\text{58}\)

See the chart for estimates.

The cost of “adtech tax” is unknown

Estimates of the percentage of advertiser spending on advertisements that does not go to the publishers who display the advertisements to their audience.\(^\text{59}\)

![Chart showing percentage of advertiser spending not going to publishers](chart.png)
AUDIENCE ARBITRAGE

- RTB arbitrages publishers’ audiences by profiling them based on their interest in the publisher’s websites & apps, and then tracking them when they leave the publisher’s properties to advertise to them cheaply when they later visit junk internet properties. From the publisher’s perspective this is a form of theft. 60

- RTB arbitrage hurts quality publishers of all sizes, including new entrants. The publisher of Recode, then a new technology news website, explained his personal experience:

  “I was seated at a dinner next to a major advertising executive. He complimented me on our new site’s quality... I asked him if that meant he’d be placing ads on our fledgling site. He said yes, he’d do that for a little while. And then, after the cookies he placed on Recode helped him to track our desirable audience around the web, his agency would begin removing the ads and placing them on cheaper sites our readers also happened to visit. In other words, our quality journalism was, to him, nothing more than a lead generator for target-rich readers, and would ultimately benefit sites that might care less about quality.” 61

- This enables a business model for junk and deprives worthy publishers of the opportunity to exclusively sell their own audience’s attention. The tech companies that run the arbitrage grab the discount.
Who benefits?

- Advertisers were promised that commercial surveillance would introduce scientific certainty and computing efficiency to their profession. This transparency and efficiency has not materialized.

- Google and Facebook colluded to advantage each other at the expense of publishers and advertisers, under their 2018 “Jedi Blue” agreement. Google and Facebook colluded to advantage each other at the expense of publishers and advertisers, under their 2018 “Jedi Blue” agreement. Irrespective of the recent finding regarding its legality, Jedi Blue reveals the extent to which the RTB system advantages tech companies at the expense of advertisers and publishers, and relies on technological opacity to mask that disadvantage and inefficiency.

- Similarly, States Attorneys Generals allege that Google’s “Project Bernanke” wrongfully netted an additional $230 million in a single year at the expense of advertisers by rigging RTB auctions on its ad exchange.

- A study of transaction data determined that surveillance-based advertising yields only a 4% premium for publishers. This estimate is likely to be incorrect because it did not factor in the cost to publishers of ad fraud and audience arbitrage.

- Many publishers including Bloomberg, The Financial Times, and The New York Times are stopping using RTB, and relying on better alternatives that do not expose people to widespread surveillance.

- Even Google now endorses the view that tracking across the Internet is not necessary for online advertising to support publishing, search, and social media.

- Commercial surveillance does not sustain publishers or serve advertisers. Nor does it sustain the open Internet. There is no countervailing benefit to publishers, advertisers, or consumers that offsets the harm to consumers.
Deception

- In February 2022, EU privacy enforcers ruled that the RTB industry\textsuperscript{70} consent pop-ups are unlawful.\textsuperscript{71} They also found that the trade body IAB Europe “was aware of risks linked to non-compliance” and “was negligent”.\textsuperscript{72}

- IAB Europe called its illegal consent pop-up system the “Transparency & Consent Framework” (TCF). It claimed the TCF gave people “control and transparency over their personal data”.\textsuperscript{73} But it did not matter what a person clicked on these consent screens: the insecurity of RTB meant that their data could still be widely shared and reused.

- This is a new form of spam. These consent popups plagued European Internet users for four years on 80\% of the internet.\textsuperscript{74}

- In 2017, a year before unleashing this wave of consent popup spam, IAB Europe’s CEO acknowledged in writing to the European Commission that RTB was legally “incompatible” with consent under the relevant law.\textsuperscript{75}

- Even so, TCF consent spam was claimed to obtain consent from 90\%+ of people after two months.\textsuperscript{76} But when Apple enabled people to decide whether they would be tracked, only 4\% of U.S. users chose to allow tracking after two months.\textsuperscript{77}

- The RTB industry has introduced variants of this same deceptive, nuisance TCF consent system across the United States.\textsuperscript{78} This is deception on a massive scale.

- The RTB industry has recently begun to pervert the term “contextual advertising” to encompass and enable continued broadcast of tracking data. In October 2022 the IAB, the tracking industry trade body, published a new definition of contextual advertising that allows for device identification.\textsuperscript{79} This reframing is deceptive and contrary to the FTC’s established definition.\textsuperscript{80}
Conclusion

- RTB demonstrates the **unfairness**, **deception**, and **serious national security hazard** of commercial surveillance.

- The Commission should take urgent and robust measures **to protect Americans**. It should **define Real-Time Bidding as an unfair and deceptive practice**.

- A **ban on surveillance advertising**, including all advertising based on a profile of a person (unless a person explicitly asks for this in a specific and limited context), should be among those measures.\(^{81}\)
Notes

Note: links may be removed over time.
If a link is inoperable then refer to the Wayback Machine of the Internet Archive for an archived version of the source.


3 The UK Competition Authority reports that Google has market power in RTB. Its position is do dominant that it can charge higher prices.

4 According to BuiltWith, checked on 11 October 2022 (URL: https://trends.builtwith.com/ads/DoubeClick.Net).


6 Calculated by dividing broadcasts per day by 90% of U.S. population (the proportion online), and dividing the result by the number of minutes the average U.S. internet user spends online per day.


8 ibid., p. 1.

9 See “lat” and “long” in “Object: Geo” in “AdCom v1, IAB TechLab”, March 2022 (URL: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.pdf#object_geo).


11 “IAB Content Taxonomy v1”, IAB TechLab (archived URL: https://iabtechlab.com/wp-content/uploads/2021/10/Content-Taxonomy-1.0.xlsx). This version of the taxonomy was supposedly “depreciated”, appears to be in use.

12 Some or all RTB ad exchanges reject bid requests unless they contain ID codes about the person who will see the ad.

abtechlab.com/standards/audience-taxonomy/) An updated version of the IAB Audience Taxonomy has been recently released, and excludes most religious and health characteristics. “Audience taxonomy 1.1”, IAB Tech Lab (URL: https://abtechlab.com/wp-content/uploads/2020/07/IABTL-Audience-Taxonomy-1.1-Final.xlsx). The previous version remains the one in general use. The recent update adds the letters “SCD” to some, but not all, items that reveal especially sensitive data, but there remains no restriction on whether these items are broadcast in the RTB system, or whether the full URL of who is viewing can be broadcast along with other data that could single them out.

14 According to the first screen of the company’s website (URL: https://www.mobilewalla.com/).
15 “Sources of mobile signal collection are … exchange supply signals.” (The word “exchange” is common industry shorthand for RTB Ad Exchange.) In “Mobilewala”, Adobe Audience Finder (archived URL: https://web.archive.org/web/20200628160602/https://www.adobe-audience-finder.com/data_partner/mobilewala/).
See also CEO Anindya Datta’s statement that “Ad requests are not only information-rich, but are also relatively easy to interpret, given the structure imposed on them by standards bodies (such as the OpenRTB organization). … Bid Requests (BRQs) … represent a key source of data helpful in modelling...” in “A largely ignored but critical dimension to incorporate in understanding consumers on mobile”, The Data Source, Oracle, Fall 2016 (https://cdn2.hubspot.net/hubfs/4309344/the-data-source-magazine-fall-2016.pdf), p. 22.
16 RTB broadcasts are also referred to as “bid stream”, “bidstream”, or “bid requests”, and sometimes as “ad requests”.
18 An engineer who worked at the company between 2014 and 2019 notes in his resume that he built on “a data segmentation product … on top of collected mobile bid stream data”.16 This refers to data broadcast in RTB bid requests. According to the same document, this was applied to “tens of terabytes of data a day”. See Resume of Jiang HaoYuan, GitHub (URL: https://haoyuan90.github.io/Resume/).
19 Mobilewalla uses RTB data to build a profile of people’s locations over time. It collects device IDs, GPS coordinates, whether the location is work or home or “other”, app in use, number of times seen at this location and/or using this app, timestamps, specific device details. See the full list in ”Mobilewalla Aggregated Data Dictionary”, Mobilewalla, 2020 (URL: https://cdn2.hubspot.net/hubfs/4309344/Content%20offers/Mobilewalla%20Data%20Dictionary_Aggregated_FEB2020.pdf).

20 See for example “Ramadan Audience Segments”, Mobilewalla (URL: https://f.hubspotusercontent40.net/hubfs/4309344/MW%20Audience%20Segments_Ramadan%202021.pdf), and “Lunar New Year Audience Segments”, Mobilewalla, (URL: https://web.archive.org/web/20221011144006/https/f.hubspotusercontent40.net/hubfs/4309344/MW%20Audience%20Segments_Ramadan%202021.pdf).
21 “We have created Ramadan audience segments using predictive modelling methods based on consumers’ mobile app usage observed during Ramadan 2020.” in “Reach your best prospects this Ramadan”, Mobilewalla, (URL: https://web.archive.org/web/20220328200602/https/cdn2.hubspot.net/hubfs/4309344/MW%20Audience%20Segments_Ramadan%202020.pdf).
22 Reach your best prospects this Ramadan, Mobilewalla, (URL: https://web.archive.org/web/20220328200602/https/cdn2.hubspot.net/hubfs/4309344/MW%20Audience%20Segments_Ramadan%202020.pdf).
26 The industry acknowledges that “there is no technical way to limit the way data is used after the data is received” in “pubvendors.json v1.0”.
27 The UK Information Commissioner’s Office (ICO) reported that “once data is out of the hands of one party, essentially that party has no way to guarantee that the data will remain subject to appropriate protection and controls” in “Update report into adtech and real time bidding”, 20 June 2019 (URL: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-d191220.pdf), pp. 20-1.
28 This was confirmed by a decision of 28 European data protection authorities. See paragraph 429, “Decision on the merits 21/2022 of 2 February 2022”, European Data

29 For example, see California Civil Code § 1798.150 (2020).

30 The word “thousands” is used in “pubvendors.json v1.0.”

31 Google’s public list of data recipients includes companies such as Beijing Fanwei Information Technology Co., Ltd., 世纪富轩科技发展（北京）有限公司 (DHgate Group), Shanghai Hecheng International Travel Co., Ltd. See “Ad Manager Certified External Vendors”, Google (URL: https://developers.google.com/third-party-ads/adx-vendors).

32 Google’s public list of data recipients includes companies such as Mail.Ru LLC, ОТМ ВОРАД ВАРА (OTM), Yandex and others. See “Ad Manager Certified External Vendors”, Google (URL: https://developers.google.com/third-party-ads/adx-vendors).

33 “Is Google sharing data from Americans and Europeans with sanctioned Russian adtech companies?”, Adalytics, 1 July 2022 (URL: https://adalytics.io/blog/sanctioned-ad-technology-data), see also “Google Allowed a Sanctioned Russian Ad Company to Harvest User Data for Months”, ProPublica, 1 July 2022 (URL: https://www.propublica.org/article/google-russia-rotation-target-otm-yandex-and-others).

34 The industry acknowledges that “there is no technical way to limit the way data is used after the data is received” in “pubvendors.json v1.0”.

35 “IAB Audience Taxonomy” v1 and v1.1.


39 “The Ease of Tracking Mobile Phones of U.S. Soldiers in Hot Spots”, Wall Street Journal, 26 April 2021 (URL: https://www.wsj.com/articles/the-ease-of-tracking-mobile-phones-of-u-s-soldiers-in-hot-spots-11619429402). The reporter confirmed that much of the data was from RTB when queried by ICCL.

51 Fake Accounts, Facebook (URL: https://transparency.fb.com/data/community-standards-enforcement/fake-accounts/facebook/).


54 See “Bot Baseline: Fraud in Digital Advertising”, White Ops and ANA, December 2014 (URL: http://www.ana.net/getfile/21853);

“Bot Baseline: Fraud in Digital Advertising”, White Ops and ANA, December 2014 (URL: http://www.ana.net/getfile/21853);

“2015 Bot Baseline: Fraud in Digital Advertising”, White Ops and ANA, January 2016 (URL: https://www.ana.net/getfile/23322);


55 See figure 2.3, “Online platforms and digital advertising: market study final report”, UK Competition & Markets Authority, 1 July 2020 (URL: https://twitter.com/LBC/status/1581960701844738049, p. 50).


57 See “Where did the money go? Guardian buys its own ad inventory”, Mediatel Newsline, 4 October 2016 (URL: https://mediatel.co.uk/newsline/2016/10/04/where-did-the-money-go-guardian-buysits-own-ad-inventory/).


59 “Where did the money go? Guardian buys its own ad inventory”, Mediatel Newsline, 4 October 2016 (URL: https://mediatel.co.uk/newsline/2016/10/04/where-did-the-money-go-guardian-buysits-own-ad-inventory/);


“Programmatic: Seeing Through the Financial Fog”, ANA, May 2017 (URL: https://www.ana.net/miccontent/show/id/44602);

“Global Ad Trends: Threats to digital advertising”, WARC (URL: https://www.warc.com/content/paywall/article/Global_Ad_Trends_March_2018_Threats_to_digital_advertising/en-GB/1211841);

“Online advertising in the UK A report commissioned by the Department for Digital, Culture, Media & Sport”, Plum Consulting, February 2019 (URL: https://plumconsulting.co.uk/wpdm-package/ian-2019-online-advertising-in-the-uk-final-report.pdf);


61 “Mossberg: Lousy ads are ruining the online experience”, The Verge, 30 January 2017 (URL: https://www.theverge.com/2017/1/18/14304276/walt-mossberg-online-ads-bad-business).

62 “Third amended complaint”, In re: Google Digital Advertising Antitrust Litigation, Civil Action No.: 1:21-md-03010-PKC, 14 January 2022 (URL: https://texasattorneygeneral.gov/sites/default/files/images/child-support/20220114._195_0_States%207th%20Amended%20Complaint.pdf), pp 141-62. The matter is also currently under investigation by the Department of Justice, the UK Competition & Markets Authority, and the European Commission.

63 Opinion and order, 21-md-3010, Docket # 217; 21-cv-6841, Docket # 176, 13 September 2022 (URL: https://www.courtlistener.com/docket/60181878/209/the-state-of-texas-v-google-llc/).


“Charting a course towards a more privacy-first web”, Google, 3 March 2021 (URL: https://blog.google/products/ads-commerce/a-more-privacy-first-web/).


Paragraph 547, “Decision on the merits 21/2022 of 2 February 2022”. See also “GDPR enforcers rule that IAB Europe’s consent popups are unlawful”, ICCL, 2 February 2022 (URL: https://www.iccl.ie/news/gdpr-enforcer-rules-that-iab-europes-consent-popups-are-unlawful/).


Author:
Dr Johnny Ryan FRHistS is a Senior Fellow at ICCL (the Irish Council for Civil Liberties) and a Senior Fellow at the Open Markets Institute. He has held senior roles in publishing, online advertising, and web browser firms. Dr Ryan is regularly invited to give expert testimony, and has appeared before the United States Senate and the European institutions.

Organisations:
The Irish Council for Civil Liberties (ICCL) is Ireland’s oldest independent human rights body. It has been at the forefront of every major rights advance in Irish society for over 40 years. We are a non-profit, independent of the Irish Government.

The Open Markets Institute is a Washington, D.C.-based non-profit that works to address threats to democracy, individual liberties, and national security from today’s unprecedented levels of corporate concentration and monopoly power. Credited by the Financial Times as “driving the debate” around the resurgence of interest in antitrust, Open Markets uses research and journalism to expose the dangers of monopolization, identifies changes in policy and law to address them, and educates policymakers, academics, movement groups, and other influential stakeholders to re-establish the competitive markets that long formed the bedrock of American democracy.

The Trans Atlantic Consumer Dialogue (TACD) is a forum of US and EU consumer organisations which develops and agrees on joint consumer policy recommendations to the US government and European Union to promote the consumer interest in EU and US policy making.

Members of the Trans Atlantic Consumer Dialogue
Members in the United States are: American Council on Consumer Interests; Americans for Financial Reform; Center for Digital Democracy; Center for Economic Justice; Center for Food Safety; Center for Media and Democracy; Center for Science in the Public Interest; Center for Study of Responsive Law; Community Nutrition Institute; Consumer Action; Consumer Federation of America; Consumer Watchdog; Economic Justice Institute; Electronic Frontier Foundation; Electronic Privacy Information Center; Federation of State Public Interest Research Groups; Institute for Agriculture and Trade Policy; International Centre for Technology Assessment; Knowledge Ecology International; National Association of Consumer Advocates; National Consumers League; Prevention Institute; Privacy Rights Clearinghouse; Public Citizen; Public Knowledge; American Economic Liberties Project; and the World Privacy Forum. Members in Europe are: ADUSBEF; Altoconsumo; Asociacion Valenciana de Consumidores y Usuarios; Associazione Consumatori Utenti; Associazione per la Difesa e l’Orientamento dei Consumatori; BEKU Pharma-Kampagne, Germany; Bulgarian National Consumers Association; Centro de Arbitrages de Conflictos de Consumo; Citizens Advice; Comité para la Difusión de la Competencia; Consumers’ Association of Ireland; Consumers’ Federation of Greece; dTest; European Community of Consumer Co-operatives; European Digital Rights; European Health Alliance; Federconsumatori; Forbrugerrådet (Danish Consumer Council); Forbrukerrådet (Norwegian Consumer Council); Health Action International; Knowledge Ecology International; Kuluttajaliitto-Konsumentförbundet ry (Consumers’ Union of Finland); Movimento Consumatori; noyb; Open Rights Group; Organizacion de Consumidores y Usuarios; Országos Fogyasztótudományi Egyesület; Privacy International; Association for the Protection of Consumers, Romania; Slovene Consumers Association; Sustain; Sveriges Konsumenter (Swedish Consumer Coalition); Swedish Consumer Co-operatives; Test – Aankoop; Test – Achat; The European Consumers’ Organisation; Tudatos Vásárlók Egyesülete; Union Fédérale des Consommateurs-UFC Que Choisir; Union Nacional de Asociaciones Españolas; Verbraucherzentrale Bundesverband; Verein für Konsumenteninformation; and Which?