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

TACD Trans Atlantic Consumer Dialogue
OPEN MARKETS LIBERTY • DEMOCRACY • PROSPERITY
Irish Council for Civil Liberties

TACD Trans Atlantic Consumer Dialogue

OPEN MARKETS

Irish Council for Civil Liberties

In this submission

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.

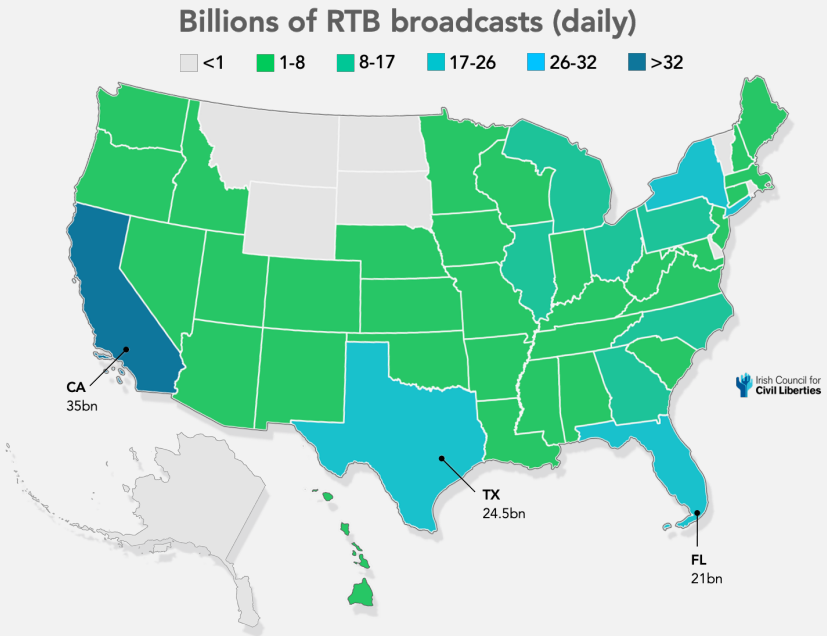
- **Google is the biggest of several major RTB companies**.[3] Its system Is live on **7.2 million websites**[4] and broadcasts data such as what people are viewing or doing on a website or app and their "hyperlocal"[5] locations **31 billion times every day in the U.S.**

- 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**.

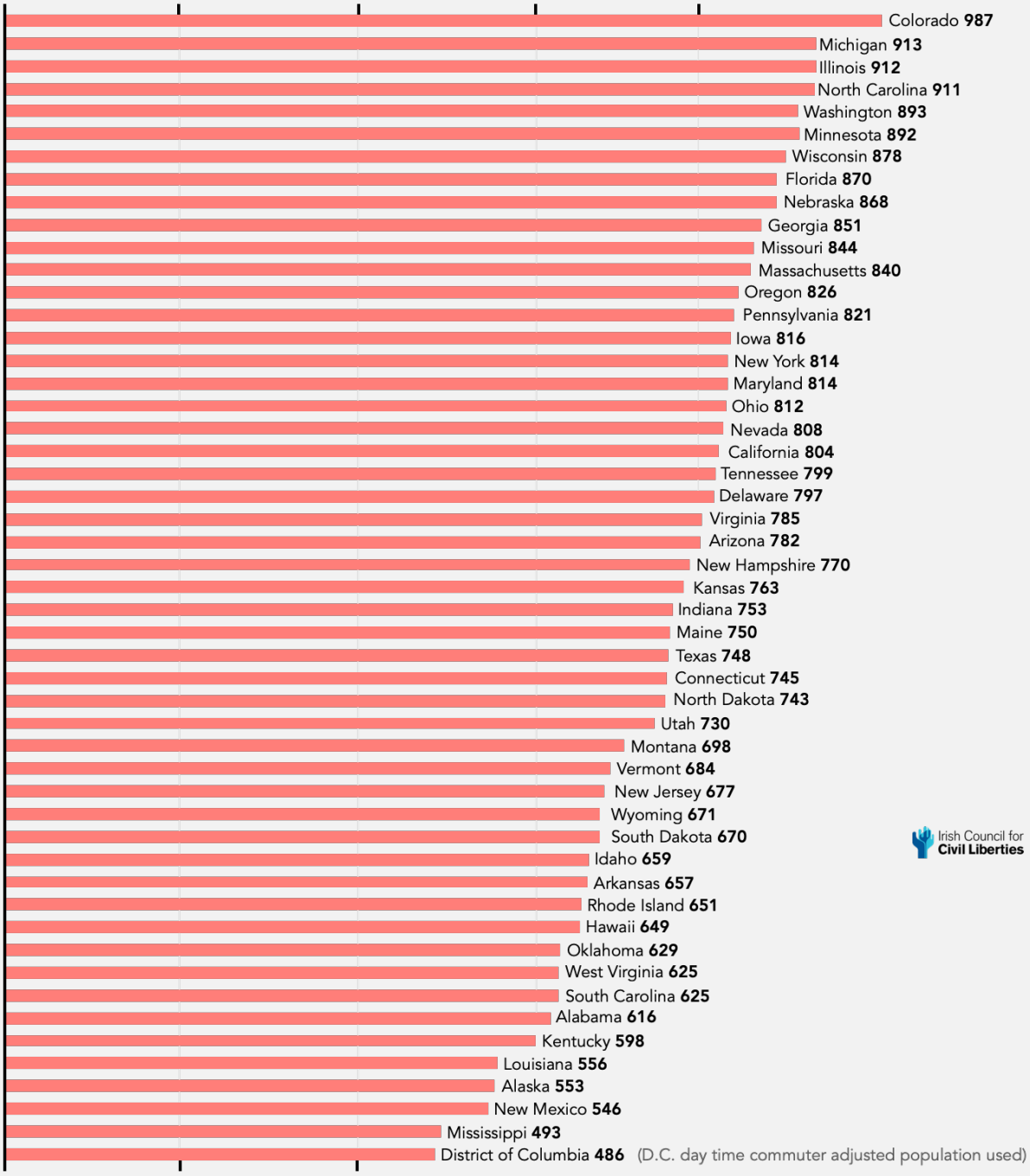
Biggest Data Breach Ever. Repeated Daily.

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.**[8] 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.



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**[9] (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.[11] 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.[12] 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**.

- The "IAB Audience Taxonomy" is the industry technical standard for data brokers' **hidden dossiers about every American**. It contains over two thousand characteristics, for example: "**Very low net worth**" (IAB code 193), "**Judaism**" (IAB 603), "**Rural**" (IAB 147), "**Conservative**" (IAB 199), "**Bail bonds**" (IAB 1495), "**Mental health**" (IAB 562), "**Online gambling**" (IAB 1540), "**STD medications**" (IAB 1580).[13]

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.[14] RTB is one of its main sources.[15] Its CEO says RTB data[16] can even show frequency of church attendance:[17]

> "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"[18] to collect people's GPS coordinates, homes, work locations and what they do on their phones.[19] It categorizes people by ethnicity[20] (for example based on their phone use during Ramadan,[21] or "were observed frequently in mosques"[22]), by income, and other intimate characteristics.[23]

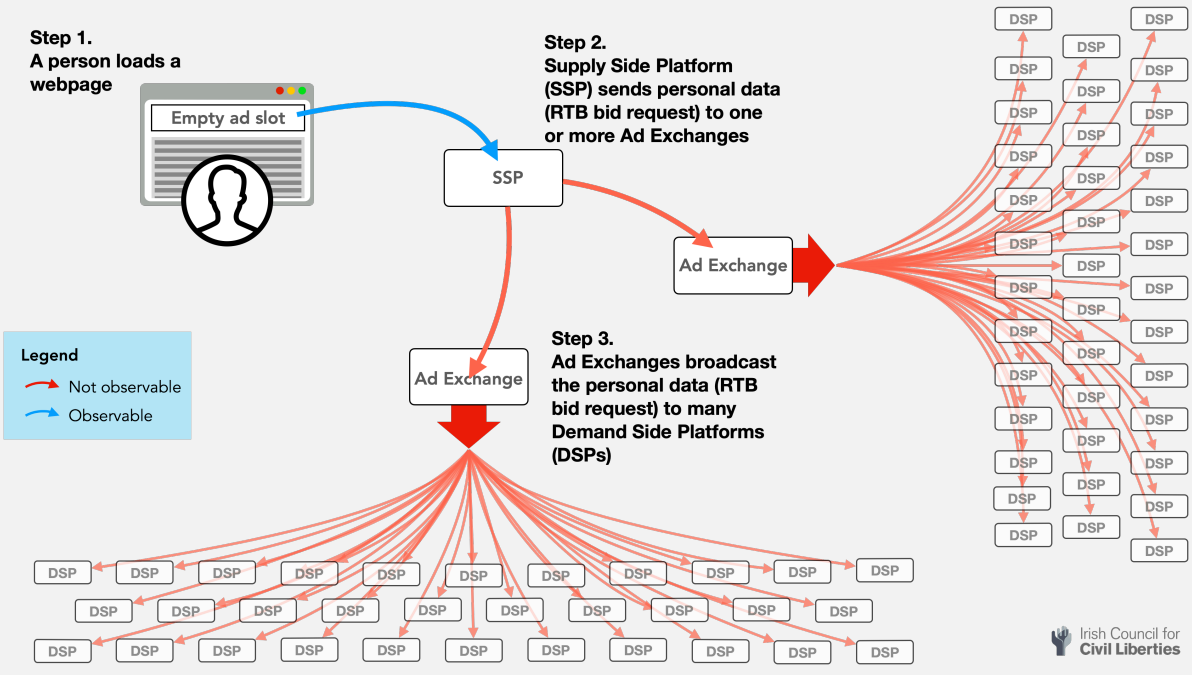
Lack of security

- 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.[24] 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.**[25] Microsoft Xandr says 1,647 firms may receive data from its Ad Exchange.[3] 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,[26] UK regulatory investigation,[27] and EU-wide enforcement action.[28] There are commercial reasons to share it widely with business partners, or anyone else who will pay. **RTB is a massive, systematic data breach**.[29]

- 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



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

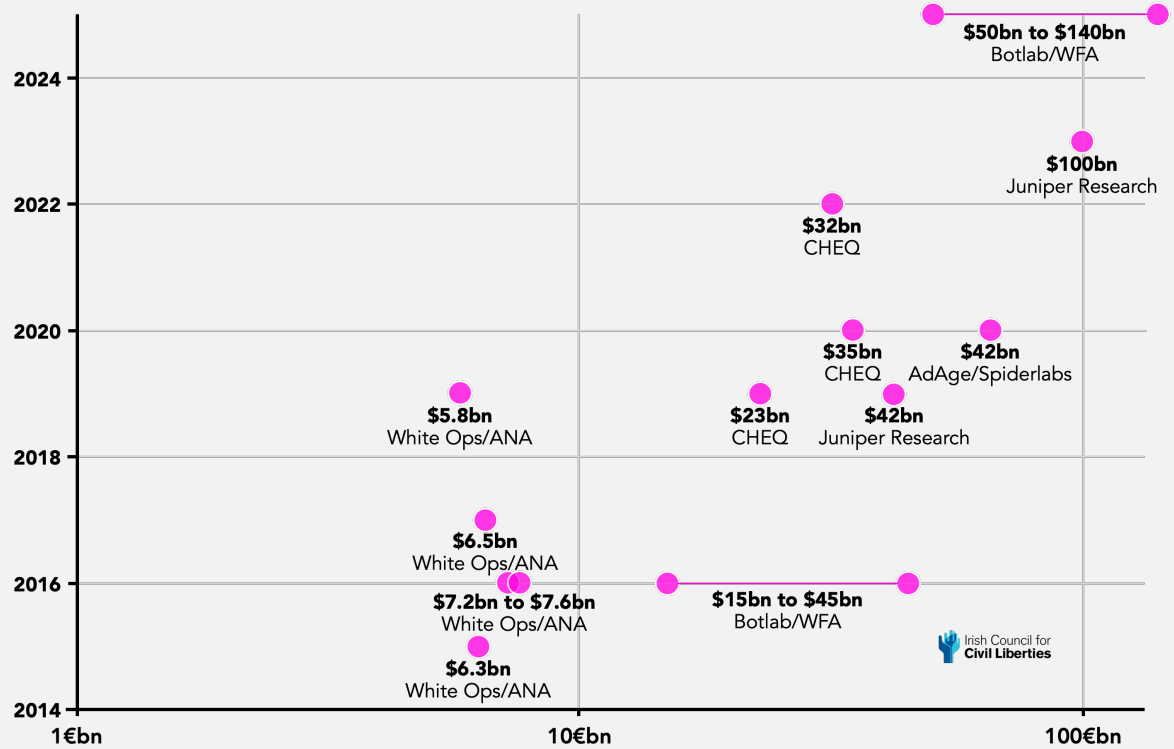
Commercial surveillance harms consumer choice by imperiling publisher sustainability in four ways.

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.**[51] For context, **Facebook claims only 2.9 billion active monthly users.**[52]
- 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.**[53]
- 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.[54]



Note: ANA estimates are for US market. Juniper, CHEQ, and WFA estimates are global.

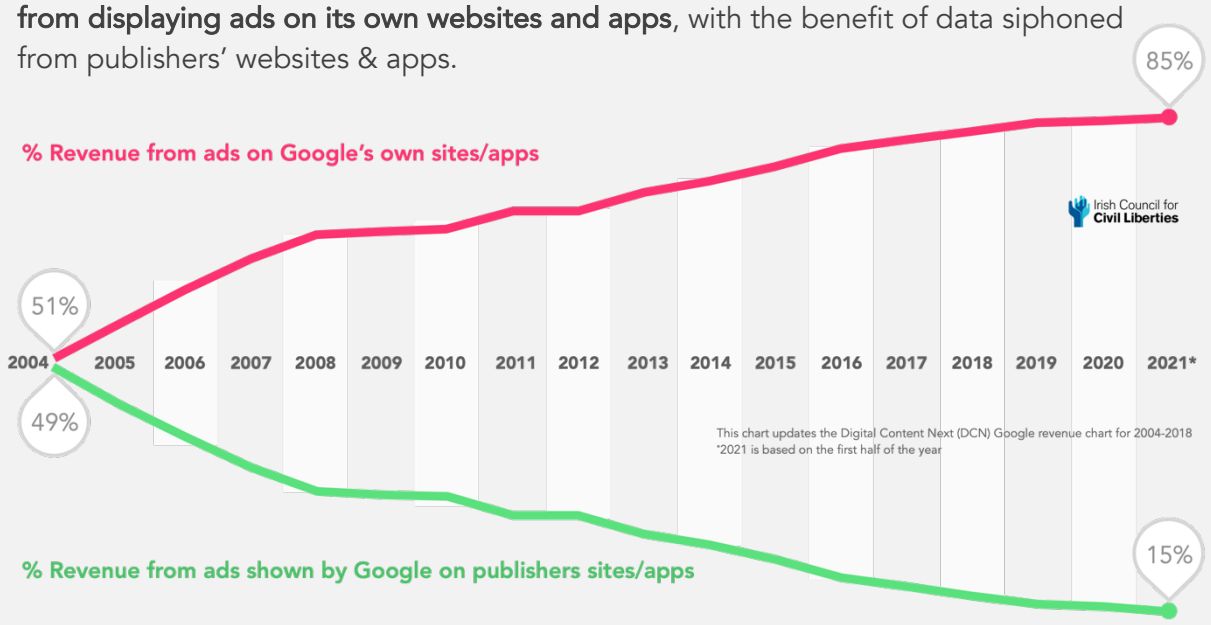
BIG TECH THEFT OF DATA FROM PUBLISHERS

- **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.



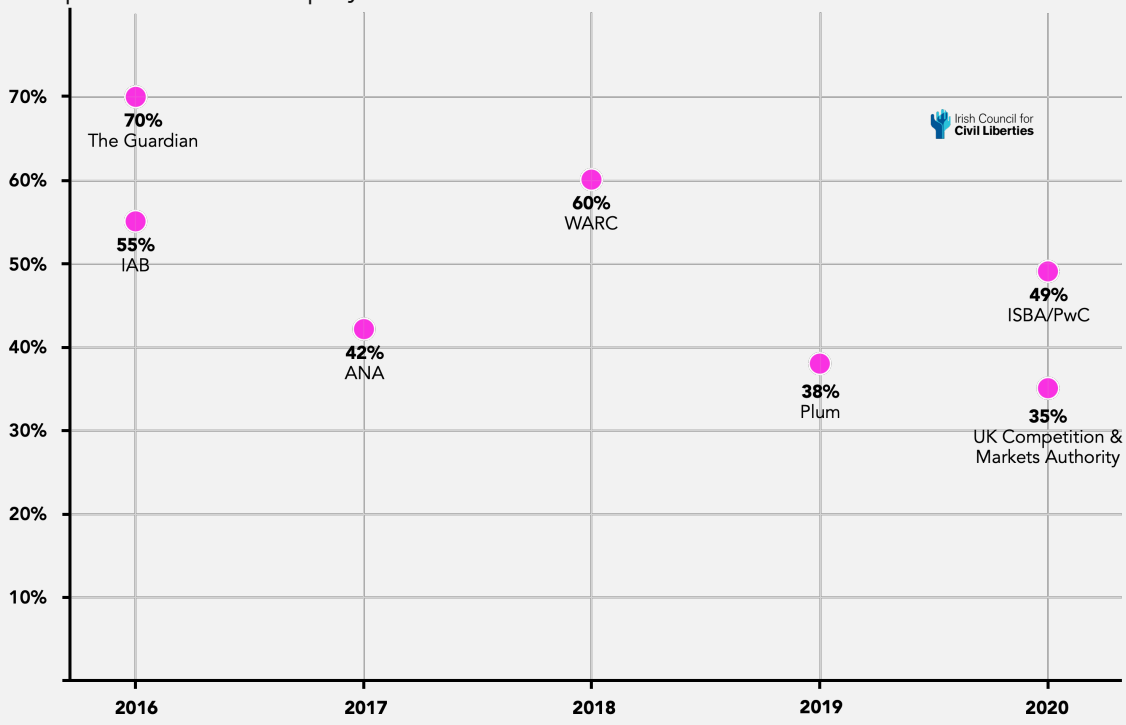
OPAQUE "ADTECH TAX"

- 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.[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.[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.[59]



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.**[62] Irrespective of the recent finding regarding its legality,[63] 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.[64]

- A study of transaction data determined that surveillance-based advertising yields **only a 4% premium for publishers**.[65] 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,**[66] **The Financial Times,**[67] **and The New York Times**[68] **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.[69]

- 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[70] consent pop-ups are unlawful.**[71] They also found that the trade body **IAB Europe "was aware of risks linked to non-compliance" and "was negligent".**[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".**[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**.[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.**[75]

- Even so, TCF consent spam was **claimed to obtain consent from 90%+** of people after two months.[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.[77]

- **The RTB industry has introduced variants of this same deceptive, nuisance TCF consent system across the United States.**[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.**[79] This reframing is deceptive and contrary to the FTC's established definition.[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.

[1] "Programmatic" including display and video ads accounted for an estimated $99bn in 2021, whereas Search accounted for an estimated $78.3bn, according to "PwC IAB Internet Advertising Revenue Report 2021", April 2022 (URL: https://www.iab.com/insights/internet-advertising-revenue-report-full-year-2021/), pp 17, 21.

[2] See "Technical report: Out of control – a review of data sharing by popular mobile apps", Norwegian Consumer Council, January 2020 (URL: https://storage.forbrukerradet.no/media/wp-content/uploads/2020/01/mnemonic-security-test-report-v1.0.pdf).

[3] The UK Competition Authority reports that Google has market power in RTB. Its position is do dominant that it can charge higher prices.
In "Online platforms and digital advertising Market study final report", UK Competition & Markets Authority, 1 June 2020 (URL: https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf) , p. 20.

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

[5] "Authorized Buyers Proto v253", Google (URL: https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide#hyperlocalset-object).

[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.

The average U.S. time on the Internet per day is 425 minutes according to survey of internet users 16 to 64, conducted by GWI in Q3 of 2021. "Digital 2022: the United States of America", We Are Social (URL: https://datareportal.com/reports/digital-2022-united-states-of-america), p. 23.

Total U.S. broadcasts per day is 294,423,672,758 according to "The Biggest Data Breach ICCL report on the scale of Real-Time Bidding data broadcasts in the U.S. and Europe", ICCL, May 2022 (URL: https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/).

The U.S. population in 2021 was 331,893,745 according to the U.S. Census (URL: https://www.census.gov/data/tables/time-series/demo/popest/2020s-state-total.html#par_textimage_1574439295).

[7] For detail on the scale of RTB see "The Biggest Data Breach ICCL report on the scale of Real-Time Bidding data broadcasts in the U.S. and Europe", ICCL, May 2022 (URL: https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/).

[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.md#object_geo).

[10] See "HyperlocalSet" in "Authorized Buyers Proto v253", Google (URL: https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide#hyperlocalset-object).

[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.
For example, Microsoft Xandr says "*Xandr only responds to a bid when we can map your request to a Xandr user ID*" In "Supply partners", Xandr (URL - archive from 29 March 2021 because the original has been removed from public view by Xandr - http://www.iccl.ie/wp-content/uploads/2022/01/K33-xandr-incoming-bid-requestssupply_partners_3-29-2021.pdf).
Similarly, Meta's RTB system, the Meta Audience Network, requires a unique "mandatory" unique ID code. In "Server-to-server bidding", Meta for Developers (URL: https://developers.facebook.com/docs/audience-network/overview/in-house-mediation/server-to-server).
See also a brief overview of the data standard for cross-referencing data at "Data Transparency Standard 1.0", IAB Tech Lab, 27 June 2019 (URL: https://iabtechlab.com/wp-content/uploads/2019/06/Data-Transparency-Standard-1.0-Final-June-2019.pdf).

[13] "IAB Audience Taxonomy" v1 and v1.1. See archived version of website (https://web.archive.org/web/20201101045842/https://i

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://iabtechlab.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 what a person 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 "Mobilewalla", Adobe Audience Finder (archived URL: https://web.archive.org/web/20200628160602/https://www.adobe-audience-finder.com/data_partner/mobilewalla/).
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".

[17] "A largely ignored but critical dimension to incorporate in understanding consumers on mobile", Oracle Data Cloud: The data source magazine, Fall 2016 (URL: https://cdn2.hubspot.net/hubfs/4309344/the-data-source-magazine-fall-2016.pdf), p. 23.

[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"*.[18] 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%20CNY%20Segments%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).

[23] For example as "expectant families, diet & weight loss, low income" in "Time: A critical dimension of understanding mobile consumers", presentation hosted at AdSquare.com, March 2017 (archive URL: https://www.iccl.ie/wp-content/uploads/2022/10/08_AIM_Mobilewalla.pdf).

[24] The word "thousands" is used in "pubvendors.json v1.0", IAB Europe, 25 April 2018 (URL: https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/pubvendors.json%20v1.0%20Draft%20for%20Public%20Comment.md#liability).

[25] See Google documentation of recipients "Ad Manager Certified External Vendors", Google (https://developers.google.com/third-party-ads/adx-vendors).

[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-dl191220.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

Protection Board (URL: https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-21-2022-english.pdf).

[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 北京泛为信息科技有限公司 (Beijing Fanwei Information Technology Co., Ltd.), 世纪富轩科技发展（北京）有限公司 (DHgate Group), 上海赫程国际旅行社有限公司 (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 **Мэйл.Ру** (Mail.Ru LLC), **ОТМ ВОРЛД ВАЙД** (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-tech-user-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-rutarget-sberbank-sanctions-ukraine).

[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.

[36] Senators Wyden, Gillbrand, Brown, Cassidy, Warner, and Warrren to CEOs of RTB companies, 1 April 2021 (URL: https://www.cassidy.senate.gov/imo/media/doc/040121%20Bidstream%20Letter%20to%20ATT.pdf).

[37] H.R. 8367 to amend the Intelligence Authorization Act for Fiscal Year 2023.

[38] "How the U.S. Military Buys Location Data from Ordinary Apps", *Vice*, 16 November 2020 (URL: https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x).

[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.

[40] "Capacity enhancement guide: securing web browsers and defending against malvertising for federal agencies", CISA, January 2021 (URL: https://www.cisa.gov/sites/default/files/publications/Capacity_Enhancement_Guide-Securing_Web_Browsers_and_Defending_Against_Malvertising_for_Federal_Agencies.pdf), p. 2.

[41] "How Cellphone Data Collected for Advertising Landed at U.S. Government Agencies", *Wall Street Journal*, 18 November 2021 (https://www.wsj.com/articles/mobilewalla-says-data-it-gathered-from-consumers-cellphones-ended-up-with-government-11637242202).

[42] Ron Wyden, Maria Cantwell, Elizabeth Warren, et. al. to Joseph J. Simmons, FTC Chairperson, 31 July 2020 (URL: https://www.wyden.senate.gov/imo/media/doc/073120%20Wyden%20Cassidy%20Led%20FTC%20Investigation%20letter.pdf).

[43] See "Suicidal gambling addict groomed by Sky Bet to keep him hooked, investigation reveals", *The Daily Mail*, 26 January 2022 (URL: https://www.thisismoney.co.uk/money/markets/article-10444901/Suicidal-gambling-addict-groomed-Sky-Bet-hooked.html) and technical report by Wolfie Christl, "Digital Profiling in the online gambling industry – technical report", Cracked Labs, January 2022 (URL: https://cdn.sanity.io/files/btrsclf0/production/6217f28e8b2360268c0a4d32dc2910897e1d639f.pdf).

[44] See ICCL submission to Irish Data Protection Commissioner, 21 September 2020 (https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-Protection-Commissioner.pdf), p. 6.

[45] "Out of Control: How consumers are exploited by the online advertising industry", Norwegian Consumer Council, January 2020 (URL: https://storage.forbrukerradet.no/media/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf), pp. 123-159.

[46] See "Grindr User Data Was Sold Through Ad Networks", *Wall Street Journal*, 2 May 2022 (https://www.wsj.com/articles/grindr-user-data-has-been-for-sale-for-years-11651492800) and related recording https://www.wsj.com/podcasts/google-news-update/grindr-users-data-could-be-purchased-through-ad-networks/ceea7c29-4dfd-4328-9183-b41f1c8d2ec0.

[47] See ICCL submission to Irish Data Protection Commissioner, 21 September 2020, 6.

[48] For information on the data and connection to the RTB bidstream see "Illinois Bought Invasive Phone Location Data From Banned Broker", EFF, 19 August 2021 (URL: https://www.eff.org/sh/deeplinks/2021/08/illinois-bought-invasive-phone-location-data-banned-broker-safegraph).

[49] According to ICCL's conversation with the EFF researchers.

[50] Congresswoman Eshoo to Chairperson Khan, 13 September 2022 (URL: https://eshoo.house.gov/sites/eshoo.house.gov/files/Rep.EshootoChairKhanFTC9.13.22.pdf).

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

[52] "Facebook Reports Second Quarter 2021 Results", Meta, 28 July 2021 (URL: https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Second-Quarter-2021-Results/default.aspx).

[53] See "2016-2017 Bot baseline: fraud in digital advertising", Association of National Advertisers (URL: https://www.ana.net/content/show/id/botfraud-2017), p. 15.

[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/23332);

"CHEQ Report: Online Ad Fraud To Cost $23 Billion Globally in 2019", PR Newswire, 3 June 2019 (https://www.prnewswire.com/news-releases/cheq-report-online-ad-fraud-to-cost-23-billion-globally-in-2019-300860628.html);

"The Economic Cost of Bad Actors on the Internet: Ad Fraud 2020", CHEQ, 2021 (URL: https://info.cheq.ai/hubfs/Research/Economic-Cost-BAD-ACTORS-ON-THE-INTERNET-Ad-Fraud-2020.pdf);

"Advertising fraud losses to reach $42 billion in 2019, driven by evolving tactics by fraudsters", Juniper Research, May 2019 (URL: https://web.archive.org/web/20220123192416/https://www.juniperresearch.com/press/advertising-fraud-losses-to-reach-42-bn-2019).

[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.

[56] "Privacy & Terms", Google, (URL: https://policies.google.com/technologies/partner-sites?hl=en).

[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/).

[58] "PwC IAB Internet Advertising Revenue Report 2021", April 2022 (URL: https://www.iab.com/insights/internet-advertising-revenue-report-full-year-2021/), p. 21.

[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/);

"The Programmatic Supply Chain Deconstructing the Anatomy of a Programmatic CPM", IAB, March 2016 (URL: https://www.iab.com/wp-content/uploads/2016/03/Programmatic-Value-Layers-March-2016-FINALv2.pdf);

"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/121186?);

"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/jan-2019-online-advertising-in-the-uk-final-report-pdf/);

"Executive Summary - Programmatic Supply Chain Transparency Study", ISBA, May 2020 (URL: https://www.isba.org.uk/knowledge/executive-summary-programmatic-supply-chain-transparency-study).

[60] A group of trade publishers published an open letter to the digital advertising industry in June 2020 complaining that their audiences were being stollen. "Open letter to the advertising industry", 16 June 2020 in "Data leakage and the bidstream", BPA (https://www.bpaww.com/wp-content/uploads/2021/11/Data-Leakage-and-the-Bidstream.pdf), p. 12-3.

[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%20Third%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/).

[64] Paragraph 317, "Third amended complaint", In re: Google Digital Advertising Antitrust Litigation, Civil Action No.: 1:21-md-03010-PKC.

[65] Marotta, Abhishek, and Acquisti, "Online Tracking and Publishers' Revenues: An Empirical Analysis", May 2019 (URL: https://weis2017.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf).

[66] "Bloomberg Media Is Shutting Off Its Open-Market Programmatic Advertising", *Adweek*, 11 October 2022 (URL: https://www.adweek.com/programmatic/bloomberg-media-programmatic-ads/).

[67] "Why the FT says open web programmatic isn't worth its attention", *Ad Exchanger*, 9 September 2022 (URL: https://www.adexchanger.com/the-sell-sider/why-the-ft-says-open-web-programmatic-isnt-worth-its-attention/).

[68] "For The New York Times, Close (And Fewer) Partnerships Are The Key In A Changing Programmatic Landscape", *Ad Exchanger*, 16 May 2022 (URL: https://www.adexchanger.com/publishers/for-the-new-york-times-close-and-fewer-partnerships-are-the-key-in-a-changing-programmatic-landscape/).

[69] "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/).

[70] The copyright notice of the "Transparency & Consent Framework" names AppNexus Inc. (now Microsoft Xandr); Conversant, LLC; DMG Media Limited; Index Exchange, Inc.; MediaMath, Inc.; Oath, Inc.; Quantcast Corp.; and, Sizmek, Inc.
in IAB Europe, "Transparency & Consent Framework, Cookie and Vendor List Format, Draft for Public Comment, v1.a", IAB Europe, 7 March 2018 (URL: https://github.com/Vindico-LR/GDPR-Transparency-and-Consent-Framework/blob/master/Draft_for_Public_Comment_Transparency%20%26%20Consent%20Framework%20-%20cookie%20and%20vendor%20list%20format%20specification%20v1.0a.pdf), p. 3.

[71] "Decision on the merits 21/2022 of 2 February 2022", European Data Protection Board (URL: https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-21-2022-english.pdf). 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/).

[72] 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/).

[73] IAB Europe, "What is the Transparency & Consent Framework?", IAB Europe (URL: https://iabeurope.eu/transparency-consent-framework/).

[74] See "IAB & IAB Tech Lab Respond with Support for OpenRTB and IAB Europe's Transparency & Consent Framework", IAB, 19 October 2020 (URL: https://www.iab.com/news/iab-iab-tech-lab-respond-with-support-for-openrtb-and-iab-europe-transparency-consent-framework/).

[75] Attachment to email from IAB Europe CEO Townsend Feehan to European Commission, 26 June 2017 (URL: https://www.iccl.ie/wp-content/uploads/2022/09/1b-IAB-2017-paper.pdf), p. 3 of attachment.

[76] "Quantcast Choice Powers One Billion Consumer consent Choices in Two Months Since GDPR", Quantcast, 31 July 2018 (URL: https://www.quantcast.com/press-release/quantcast-choice-powers-one-billion-consumer-consent-choices/).

[77] "App Tracking Transparency Opt-In Rate - Monthly Updates", Flurry, 2 May 2022 (URL: https://www.flurry.com/blog/att-opt-in-rate-monthly-updates/).

[78] Called the "CCPA Framework" and "Global Privacy Platform".
See "IAB Tech Lab Finalizes Global Privacy Platform and Advises the Industry to Prepare for Updated US State-Level Signaling", IAB TechLab, 28 September 2022 https://iabtechlab.com/blog/iab-tech-lab-finalizes-global-privacy-platform/); and "Global Privacy Platform", IAB TechLab (URL: https://iabtechlab.com/gpp/).

[79] See new definition of contextual advertising in "IAB Privacy Multi Party State Agreement draft for public comment", IAB, 13 October 2022 (URL: https://www.iabprivacy.com/DRAFT+IAB+Multi-State+Privacy+Agreement+(MSPA)+-+October+2022.pdf).

[80] "FTC staff report: self-regulatory principles for online behavioral advertising", FTC, February 2009 (URL: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf), p. iii.

[81] "Resolution on Banning Surveillance-Based Advertising", Trans Atlantic Consumer Dialogue, 1 June 2022 (URL: https://tacd.org/wp-content/uploads/2022/06/20220601-TACD-Surveillance-based-Ads-Resolution-FINAL.pdf).

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; Altroconsumo; Asociacion Valenciana de Consumidores y Usuarios; Associazione Consumatori Utenti; Associazione per la Difesa e l'Orientamento dei Consumatori' BUKO Pharma-Kampagne, Germany; Bulgarian National Consumers Association; Centro de Arbitragem de Conflictos de Consumo; Citizens Advice; Comitato CODACONS; Compassion in World Farming; Confederación de Consumidores y Usuarios; Consommation, Logement et Cadre de Vie; Consumentenbond; Consumer Protection Centre; Consumers' Association of Ireland; Consumers' Federation of Greece; dTest; European Association for the Coordination of Consumer Representation; European Community of Consumer Co-operatives; European Digital Rights; European Public Health Alliance; Federconsumatori; Forbrugerraadet (Danish Consumer Council); Forbrukerradet (Norwegian Consumer Council); Health Action International; Knowledge Ecology International Europe; Kuluttajaliitto-Konsumentförbundet ry (Consumers' Union of Finland); Movimento Consumatori; noyb; Open Rights Group; Organizacion de Consumidores y Usuarios; Országos Fogyasztóvédelmi Egyesület; Privacy International; Association for the Protection of Consumers, Romania; Slovene Consumers Association; Sustain; Sveriges Konsumenter (Swedish Consumers' Association); Sveriges Konsumenter i Samverkan (Swedish Consumer Coalition); Swedish Consumer Co-operatives; Test – Aankoop / Test – Achats; The European Consumers' Organisation; Tudatos Vásárlók Egyesülete; Union Fédérale des Consommateurs-UFC Que Choisir; Union Nacional de Asociaciones Espanolas; Verbraucherzentrale Bundesverband; Verein für Konsumenteninformation; and Which?

TACD Trans Atlantic Consumer Dialogue

OPEN MARKETS LIBERTY • DEMOCRACY • PROSPERITY

Irish Council for Civil Liberties