FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of Google's RTB practices

Complaint and Request for Investigation, Injunction, Penalties, and Other Relief

Submitted by

The Electronic Privacy Information Center (EPIC) and
Irish Council for Civil Liberties (ICCL) Enforce

I. Summary

1. This complaint[1] concerns Google's failure to ensure that its Real Time Bidding ("RTB") system complies with the Protecting Americans' Data from Foreign Adversaries Act ("PADFAA") and Section 5 of the Federal Trade Commission Act. Google is overwhelmingly dominant in internet advertising. Its RTB system collects troves of personally identifiable sensitive data about United States individuals from other businesses. That data reveals Americans' employment with the military and intelligence community, locations, political views, financial problems, health, sexuality, ethnicity, and online behavior. Google's RTB system then makes this data accessible to foreign adversary countries, both directly and indirectly. As this complaint will show, the movements and vulnerabilities of America's national security decision makers, active military personnel, defense logistics workers, and even judges are available to foreign adversaries as a result. This exposes America's most sensitive institutions and industries to hacking, blackmail, and compromise by foreign and non-state actors.

2. As shown below, Google CEO Sundar Pichai was aware of the security flaws of its RTB system and did not remedy them. Internal Google communications show that senior Google executives knew about the RTB security problem for over a decade.

3. Google's own documents attest to its practice of directly sharing Americans' personally identifiable sensitive data to foreign adversary countries. In addition, Google fails to provide any evidence that it adequately vets its third-party affiliates or employs sufficient controls to ensure that Americans' personally identifiable sensitive data is not accessed by foreign adversary countries indirectly. Even if Google were to change its practices and only initially broadcast RTB data to entities in the United States, that data would

[1] EPIC Clerk Vaishali Nambiar contributed to this complaint.

inevitably become available to foreign and non-state actors because Google has no way to control what happens to the data that it broadcasts so freely. As a result, a large number of entities receive extraordinarily sensitive RTB data about America's leaders and sensitive defense personnel. This national security crisis[2] compounds the existing online tracking that has harmed Americans for decades.

4. Google's RTB practices are also unfair. The massive volume of data broadcast by Google's RTB system and the sensitivity of the data involved expose people to significant injury. As Commissioner Holyoak has aptly noted, the collection and processing of sensitive data creates particularly acute risks for consumers.[3] The ubiquity of its RTB system, and the frequency of its RTB broadcasts, make it prevalent and unavoidable.

5. These practices are deceptive. Google has a long history of hiding harmful data practices behind complicated, opaque walls and velveteen phrasing that prevents consumers from understanding what happens to their data.[4] Obfuscation has historically helped Google avoid regulation, harming competition, consumers, and national security.

---

[2] Johnny Ryan & Wolfie Christl, *America's Hidden Security Crisis: How Data about United States Defence Personnel and Political Leaders Flows to Foreign States and Non-state Actors*, Enforce at 4, 7 (Nov. 2023), https://www.iccl.ie/wp-content/uploads/2023/11/Americas-hidden-security-crisis.pdf [hereinafter Enforce Report].

[3] Commissioner Holyoak recently expressed a preference for enforcement actions that protect sensitive personal data, saying "We are more likely to find harm to consumers from mishandling of children's personal data or precise geolocation data revealing consumers' political or religious activities than we are from data practices involving less sensitive information." *Oral remarks of Commissioner Holyoak, A Path Forward On Privacy, Advertising, And AI*, Remarks at National Advertising Division Keynote 2024 (Sept. 17, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Holyoak-NAD-Speech-09-17-2024.pdf.

[4] *See* Matthew Barakat, *Google Faces A New Antitrust Trial After Ruling Declaring Search Engine A Monopoly*, AP News (Sept. 9, 2024), https://apnews.com/article/google-antitrust-ad-tech-virginia-opening-7a19f525287f782609a5316b1fdb08f0; Sara Merken, *Google Privacy Lawsuit Over Ad Bidding Process To Go Forward*, Reuters (June 14, 2022), https://www.reuters.com/legal/litigation/google-privacy-lawsuit-over-ad-bidding-process-go-forward-2022-06-14/; EPIC Amicus Brief in *Calhoun, et al. v. Google*, EPIC (Dec. 2023), https://epic.org/documents/calhoun-et-al-v-google/; Johana Bhuiyan, *Google Promised To Delete Location Data On Abortion Clinic Visits. It Didn't, Study Says*, The Guardian (Jan 17, 2024), https://www.theguardian.com/technology/2024/jan/16/google-keeps-location-history-data-abortion-clinics-despite-delete-pledge; *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*, Fed. Trade Comm'n Press Release (Sept. 4, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law; *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, Fed. Trade Comm'n Press Release (Aug. 9, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented-privacy-assurances-users-apples.

6. The national security threat posed by Google's unfair and deceptive RTB practices requires urgent investigation by the Commission.

II. Parties

7. The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, DC. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC has played a leading role in developing the authority of regulators to safeguard the rights of consumers, ensure the protection of personal data, and address privacy violations.

8. Enforce is a unit of the Irish Council for Civil Liberties ("ICCL") that advocates, investigates, and litigates to defend human rights in digital issues. ICCL is Ireland's oldest independent civil liberties and human rights body and was at the forefront of every major rights advance in Irish society for over 40 years. ICCL Enforce has investigated Google's RTB system for several years.

9. Google LLC, a Delaware corporation headquartered in California, operates as a subsidiary of Alphabet Inc. Google provides a range of services in the technology market —with a significant portion of its business concentrated on online advertising. Google dominates the RTB market. The Department of Justice estimates that Google's RTB business has 87% of the U.S. publisher ad serving market and has 88% of the ad buyer market.[5] Google RTB operates on 35.4 million websites,[6] 91% of Android apps, and 75% of iOS apps.[7] In the digital ad ecosystem, Google is a data broker because it transfers individuals' data that Google did not collect directly from those individuals.[8]

10. The Federal Trade Commission (FTC) is an independent agency of the United States government given statutory authority and responsibility by, inter alia, the FTC Act, 15 U.S.C. §§ 41-58. The Commission is charged, inter alia, with enforcing section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair and deceptive acts or practices in or affecting commerce. The Commission is also charged with enforcing the Protecting Americans' Data from Foreign Adversaries Act of 2024, ("PADFAA") "in the same

---

[5] See buy side and sell side market shares on slide 2 of Plaintiff's Closing Argument in *United States et al v. Google LLC*, 1:23-Cv-00108, (E.D. Va. 2023), https://www.justice.gov/atr/media/1378386/dl?inline.
[6] *DoubleClick.Net Usage Statistics*, BuiltWith (last visited Jan. 9, 2025), https://trends.builtwith.com/websitelist/DoubleClick.Net.
[7] *The Most Popular Ads & Monetization SDKs*, AppFigures (last visited Jan. 9, 2025), https://appfigures.com/top-sdks/ads/all.
[8] Protecting Americans' Data from Foreign Adversaries Act of 2024, 15 U.S.C. § 9901(c)(3)(A) [hereinafter PADFAA] ("'[D]ata broker' means an entity that, for valuable consideration, sells, licenses, rents, trades, transfers, releases, discloses, provides access to, or otherwise makes available data of United States individuals that the entity did not collect directly from such individuals to another entity that is not acting as a service provider.").

manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act[.]"[9]

III. Factual Background

A. How Google's Real-Time Bidding (RTB) Works

11. RTB is a digital auction process, held billions of times each day, that facilitates the buying and selling of ads on a per-impression basis.[10] Often when a user loads new content on a website or application, RTB "ad exchange" auctions take place to determine what advertisements users receive.[11]

12. Google provides that each auction occurs as a webpage or app is loading, in under 100 milliseconds.[12]

13. There are two sides to an RTB auction. Google's public glossary defines them as follows:

- "Demand-side platform (DSP): System enabling advertisers to manage multiple ad exchanges from a single interface."

- "Sell-side [or "supply-side] platform" (SSP): System enabling publishers to manage ad impression inventory and maximize revenue from digital media."[13]

14. The two sides are connected by ad exchanges. Google's public documentation describes them as follows:

> "An ad exchange is an online, auction-driven marketplace where ad impressions are bought and sold in real time. Just like ad networks and yield managers, an ad exchange connects buyers with publishers looking to sell their ad inventory."[14]

---

[9] PADFAA, 15 U.S.C. § 9901(b)(2)(A).
[10] Enforce Report, *supra* note 2.
[11] *Authorized Buyers Overview*, Google Authorized Buyers Help (last visited Jan. 9, 2025), https://support.google.com/authorizedbuyers/answer/6138000.
[12] *Authorized Buyers Overview*, Google Authorized Buyers Help (last visited Jan. 9, 2025), https://support.google.com/authorizedbuyers/answer/6138000.
[13] *Glossary*, Google Authorized Buyers Help, Google (last visited Jan. 9, 2025), https://support.google.com/authorizedbuyers/answer/6142666?hl=en&ref_topic=21122&sjid=14896112693583045422-NA.
[14] *Authorized Buyers Overview*, Google Authorized Buyers Help (last visited Jan. 9, 2025), https://support.google.com/authorizedbuyers/answer/6138000.

15. Google's RTB system is called Authorized Buyers. Google describes it thus:

> "Authorized Buyers (formerly DoubleClick Ad Exchange) connects ad networks, agencies, and demand-side platforms with real-time inventory."[15]

The data are not collected directly from the person concerned and are sent to other entities that are not acting as a service provider to the person concerned.

16. Google's public documentation states that when a person loads a website or uses an app, an SSP sends sensitive user data to advertising exchanges in a process known as a "bid request."[16] Google may be the SSP itself or it may be one of the advertising exchanges that receives the bid request.

17. A bid request typically contains data about the person who is about to be shown an advertisement, to solicit bids from prospective advertisers for the opportunity to have their ad inserted into the ad slot that the person is about to be shown.

18. The information in a bid request can include what the person is currently doing online, where they are, and identification codes to tie this information to existing dossiers about them.[17] This is described in the next section.

19. After receiving a bid request, Google's advertising exchange will broadcast the bid request onto several DSPs. The DSPs will then examine the data and decide whether to make a bid on behalf of their client to have an ad appear in front of that exact person. DSPs also add the new data to their existing dossiers about the person.[18]

20. Several companies' advertising exchanges may receive the same bid request from an SSP, so that each of them can then run their own auction, further broadcasting the bid request. This auction-of-auctions maximizes the number of potential bids and the proliferation of RTB data about the person concerned.

21. Google's documentation describes a related process called "cookie matching" in which DSPs synchronize cookies they have previously attributed to a user with the Advertising

---

[15] *Authorized Buyers*, Google (last visited. Jan. 9, 2025), https://developers.google.com/authorized-buyers.
[16] *Real-time bidding for developers*, Google Authorized Buyers Help, https://support.google.com/authorizedbuyers/answer/6146609?hl=en; *Real-time Bidding*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/rtb/start.
[17] *OpenRTB Integration*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/rtb/openrtb-guide https://developers.google.com/authorized-buyers/rtb/openrtb-guide.
[18] Enforce Report, *supra* note 2, at 5.

Exchange's distinct cookies to identify the user.[19] Advertisers can upload their data about people to Google, and Google will reconcile that data about each person with what it receives from websites and apps and other companies.[20]

B. The Personally Identifiable Sensitive Data Shared by Google RTB

22. According to Google's own technical documentation, Google's RTB system shares bid requests that contain "details about the human user of the device; the advertising audience."[21]

23. Google's RTB technical specification says several times that "at least one" of the following two identifiers should be assigned to a person and included in bid requests about them:[22]

    - "id": Google describes this identifier as an "exchange-specific ID for the user." Google says this identifier must be assigned to the person for "long enough to serve reasonably as the basis for … retargeting."

    - "buyeruid" (Buyer User Identifier): Google's technical documentation describes the buyer user ID as a "Buyer-specific ID for the user as mapped by the exchange for the buyer."[23] Google says that it communicates "cookie match" data using this identifier, so that a company that has an existing profile about the person concerned can update their profile with new info from Google's RTB bid requests.[24]

24. Google says its bid requests use "mobile advertising identifiers" (MAID), which Google's documentation refers to as a "Platform device ID."[25] This MAID is hashed, but

---

[19] *Cookie Matching*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/rtb/cookie-guide.
[20] *See, e.g.*, *REST Resource: buyers.userLists*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/apis/realtimebidding/reference/rest/v1/buyers.userLists.
[21] *OpenRTB Integration: BidRequest*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/rtb/openrtb-guide#bidrequest.
[22] *OpenRTB Integration: User*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/rtb/openrtb-guide#user.
[23] *OpenRTB Integration: User*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/rtb/openrtb-guide#user.
[24] "Google will send you the hosted match data you matched with their Google User ID. In Google's OpenRTB implementation, BidRequest.user.buyeruid will specify this as a web-safe base64-encoded string." *Cookie Matching*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/rtb/cookie-guide.
[25] *OpenRTB Integration: Device*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/rtb/openrtb-guide#device.

Google's provides instructions on how to decrypt it.[26] Google promotes the use of MAIDs.[27]

25. When none of the previous three identifiers are available, Google says it sends what it calls "publisher provided identifiers" in bid requests.[28]

26. Google's technical documentation says it is "highly recommended" that websites and apps should provide details about what a person is viewing on the website or app to be included in its bid requests.[29] It says this can be the precise URL a person is viewing on a website, or what app they are using and what content it contains, or what they are listening to, or some information about what video they are watching.

27. Google provides for data broker classifications about the user. It says its bid requests may include codes from the IAB TechLab Audience Taxonomy.[30] This is a list of over 1,999 characteristics or categories that a person can be defined by. For example, category code 885 denotes a person who works in Aerospace and Defense procurement.[31] Other codes denote a person's income, mortgage, or financial problems. For example, IAB Audience Taxonomy code 1395 denotes "Payday and Emergency Loans[.]"[32]

28. Google also provides for classifications of what content the person is viewing. Google's documentation says it uses IAB Tech Lab Content Taxonomy (versions 2.2 and 3.0),

---

[26] *Decrypting Advertiser Identifiers for Ad Networks*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/rtb/response-guide/decrypt-device-id-ano.
[27] *See Google's Discussion of the Benefits of MAIDs in Mobile Advertising IDs*, Google Ad Manager Help https://support.google.com/admanager/answer/6274238?hl=en#pubs.
[28] *Publisher-provided Identifiers*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/rtb/openrtb-guide#publisher-provided-identifiers.
[29] "There are also several subordinate objects that provide detailed data to potential buyers. Among these are the Site and App objects, which describe the type of published media in which the impressions appear. These objects are highly recommended[.]" *BidRequest*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/rtb/openrtb-guide#app, and https://developers.google.com/authorized-buyers/rtb/openrtb-guide#site and #app and #publisher and #content.
[30] *DataExt*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/rtb/openrtb-guide#dataext.
[31] "Purchase intent" in the "Aerospace and Defense" InteractiveAdvertisingBureau Audience Taxonomy 1.1.tsv, https://github.com/InteractiveAdvertisingBureau/Taxonomies/blob/main/Audience%20Taxonomies/Audience%20Taxonomy%201.1.tsv?plain=1 (last visited Jan. 8, 2025).
[32] InteractiveAdvertisingBureau Audience Taxonomy 1.1.tsv, https://github.com/InteractiveAdvertisingBureau/Taxonomies/blob/main/Audience%20Taxonomies/Audience%20Taxonomy%201.1.tsv?plain=1 (last visited Jan. 8, 2025).

which exist for this purpose.[33] This taxonomy is a list of several thousand categories of content. As the following example codes show, this reveals much about the person:[34]

- IAB Content Taxonomy code 65 denotes "bankruptcy"
- IAB Content Taxonomy code 122 denotes "defence industry"
- IAB Content Taxonomy code 181 denotes "casinos and gambling"
- IAB Content Taxonomy code 189 denotes "divorce"
- IAB Content Taxonomy code 308 denotes "sexual conditions"
- IAB Content Taxonomy code 301 denotes "mental health"
- IAB Content Taxonomy code 314 denotes "cancer"
- IAB Content Taxonomy code 311 denotes "substance abuse"
- IAB Content Taxonomy code 462 denotes "Judaism"

29. Advertisers that use Google Ads API to buy Google RTB ad space[35] also appear to have access to Google's own Topics list of several thousand categories of content that a person is viewing. This includes content categories that reveal sensitive characteristics of the person, such as an interest in content about "AIDS & HIV."[36] Google's category "Law & Government/Military" is broken down into specific verticals like Air Force, Army, Marines, Navy, and Veterans.[37]

30. Google says its bid requests also include the person's location, expressed as latitude and longitude.[38] Google claims that it makes this data coarse, but does not reveal the extent of that coarsening.[39] It is not known to us whether this is within a range of 1,850 feet or less, as stipulated in PADFAA § 9901(c)(6)(B).

31. Bid requests also include details about the person's device, according to Google.[40] This includes "User agent" information about the software running on the device and the

[33] *DataExt*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/rtb/openrtb-guide#dataext.
[34] InteractiveAdvertisingBureau / Taxonomies, Content Taxonomy 2.2.tsv, https://github.com/InteractiveAdvertisingBureau/Taxonomies/blob/main/Content Taxonomies/Content Taxonomy 2.2.tsv (last visited Jan. 8, 2025).
[35] *How Authorized Buyers Work With Google Ad Manager*, Google Ad Manager, https://admanager.google.com/home/resources/how_authorized_buyers_work_with_google/.
[36] *See* Criterion ID 625, *Topics*, Google Ads API, https://developers.google.com/google-ads/api/data/topics (last visited Jan. 8, 2025).
[37] *See* Criterion IDs 1247-1249, 793, *Topics*, Google Ads API, https://developers.google.com/google-ads/api/data/topics (last visited Jan. 8, 2025).
[38] *Geo*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/rtb/openrtb-guide#geo.
[39] *Geographical Targeting*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/rtb/geotargeting.
[40] *Device*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/rtb/openrtb-guide#device.

version of that software, which allow the device and its user to be more easily singled out and monitored.

32. In addition, Google's documentation says its bid requests include data about the person that are provided by other data brokers. Google's documentation says segment data are provided from the data brokers including SalesForce, Oracle, LiveRamp, Nielsen, and Adobe.[41]

33. Finally, Google says it also sends other data about the person and their online activity that are provided by the website or app publisher.[42]

34. The Presidential Executive Order published on February 28, 2024 made clear that such data expose U.S. military and intelligence personnel:[43]

> Countries of concern can use their access to Americans' bulk sensitive personal data and United States Government-related data to track and build profiles on United States individuals, including Federal employees and contractors, for illicit purposes, including blackmail and espionage… Countries of concern can use AI to target United States persons for espionage or blackmail by, for example, recognizing patterns across multiple unrelated datasets to identify potential individuals whose links to the Federal Government would be otherwise obscured in a single dataset.

[41] *OpenRTB Integration*, Google Authorized Buyers, https://developers.google.com/authorized-buyers/rtb/openrtb-guide#segment (Krux Digital [SalesForce], BlueKai (Oracle), Lotame, BrightTag (Signal), LiveRamp, Ezakus, Eulerian, Adobe, Weborama, Neodata, Neustar (CRM), MParticle, Ziff Davis DBM, Publicis Media, Tealium, Modulo/AudienceOne, Accordant, The ADEX, EBay Advertising, Netsprint, Exelate (Nielsen), 1plusX.com, Emetriq, Turbo Adv, Mediarithmics, Adform, Acxiom APAC, Agora SA, AntVoice, Treasure Data, digitalAudience (socialAudience), M1 (Merkle), Segment, Acxiom, Permutive, Rudderstack, Covatic, and Piano). See also Google's list at https://storage.googleapis.com/adx-rtb-dictionaries/data_providers.txt, which Google provides as a link in its RTB documentation https://developers.google.com/authorized-buyers/rtb/openrtb-guide#data.

[42] These are called "publisher provided signals." *See About publisher provided signals (Beta*), Google (last visited Oct. 17, 2024), https://support.google.com/admanager/answer/12451124.

[43] *Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*, The White House (Feb. 28, 2024), https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.

35. The Director of National Intelligence confirms that the United States intelligence community purchases RTB data for much the same purpose.[44]

C. RTB Releases Data at Massive Scale and Without Protections, Making It Available to Foreign Adversaries by Directly Sharing and Indirectly Releasing

Direct sharing

36. Senators Cassidy, Wyden, Gillibrand, Warner, Brown and Warren asked Google what foreign companies it sends Americans' data to. Google refused to say, citing non-disclosure agreements.[45]

37. Google's own public documentation appears to admit in the plainest terms that it directly shares RTB data with companies controlled by foreign adversary countries.[46] Google maintains a public list of 2,365 companies that it states it has "certified" to receive its RTB bid requests.[47] These companies include ad exchanges and DSPs that receive RTB data directly from Google, DMPs that exchange profile data with Google, and various other companies that can surveil the person concerned including "analytics" companies that conduct invasive measurement on the page or app to examine, for example, that an ad has been seen by the targeted individual. Many are based outside the United States. For example, twelve of these Google-certified companies have the word "Beijing" in the title.

38. In the same list Google also states that it sends RTB data to "Shenzhen Tencent Computer Systems Company Limited."[48] Tencent, and its product WeChat, is the subject of an Executive Order from President Trump that prohibited the transfer of Americans' data:[49]

> Not later than 45 days after the date of this order, the Secretary, in consultation with the Attorney General and the Director of National Intelligence, shall provide a report to the Assistant to the President for

---

[44] *Office of the Director of National Intelligence Senior Advisory Group Panel on Commercially Available Information: U.S. Director of National Intelligence*, ODNI at 4-5 (Jan. 27, 2022), https://www.odni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf.

[45] *Google Response to Sen Wyden re Bidstream Data*, Google (May 4, 2021) https://www.documentcloud.org/documents/21052489-google-response-to-sen-wyden-re-bidstream-data/.

[46] Enforce Report, *supra* note 2, at 8.

[47] *Ad Manager Certified External Vendors*, Google Third-Party Ad Serving Certifications, https://developers.google.com/third-party-ads/adx-vendors.

[48] *Id.*

[49] *Executive Order on Addressing the Threat Posed by WeChat*, The White House (Aug. 6, 2020) https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/.

> National Security Affairs with recommendations to prevent the sale or transfer of United States user data to, or access of such data by, foreign adversaries, including through the establishment of regulations and policies to identify, control, and license the export of such data.

39. A separate public list maintained by Google itemizes 285 companies that Google says are "eligible to receive bid requests compliant with U.S. state privacy laws[.]"[50] That list also contains foreign companies, including companies controlled by foreign adversary countries.

40. Despite this, Google does not appear to have set any strict requirements about who can operate a DSP. In 2022, it was revealed that Google provided data to RuTarget, which also operates under the name Segmento, and which is owned by Sberbank.[51] Both RuTarget and Sberbank were at that time on the Department of the Treasury sanctioned list. Similarly, Enforce's 2023 investigation revealed that a Russian firm that sells data about Russians who visit Russian political opposition websites had been listed by Google as one of its RTB data recipients for years before Google cut Russian firms off from its direct data staring.[52]

41. Another foreign surveillance firm operated a DSP for the purpose of acquiring Google RTB data for its system surveilling "all internet users in a country[.]"[53] As Bloomberg reported, this firm harvested Google RTB data for years to power a system that "could home in on a particular building and identify who was there on a given day or time going back several months."[54] Another foreign firm cited Google's RTB system as a direct data source in its marketing material.[55]

42. Google claims the right to conduct what it calls an "audit" of each company's use of its RTB system. It is not known whether such an audit is intended to determine what a company does with the vast quantities of Americans' data that Google has sent them. If

---

[50] *Vendors Eligible to Receive Bid Requests Compliant with US States Privacy Laws*, Google Ad Manager Help, https://support.google.com/admanager/answer/10634320?hl=en.
[51] *Is Google sharing data from Americans and Europeans with sanctioned Russian adtech companies?*, Adalytics https://adalytics.io/blog/sanctioned-ad-tech-user-data; *Google Allowed a Sanctioned Russian Ad Company to Harvest User Data for Months*, ProPublica, July 1, 2022 https://www.propublica.org/article/google-russia-rutarget-sberbank-sanctions-ukraine.
[52] Enforce Report, *supra* note 2 at 8.
[53] Enforce Report, *supra* note 2 at 9 (*citing ECHO – Global Virtual SIGINT System*, Rayzone Group (archived July 24, 2021), https://rayzone.com/echo-global-virtual-sigint-system/ [permalink: https://web.archive.org/web/20210724230515/https://rayzone.com/echo-global-virtual-sigint-system/]).
[54] Ryan Gallagher, *Your Ad Data Is Now Powering Government Surveillance*, Bloomberg BusinessWeek (May 11, 2023), https://www.bloomberg.com/news/articles/2023-05-11/surveillance-company-turns-ad-data-into-government-tracking-tool.
[55] Enforce Report, *supra* note 2 at 10, 13 (citing *Patternz: National Security Pattern Detection*, ISA Security (archived June 22, 2021), http://isasecurity.org/patternz [permalink: https://web.archive.org/web/20210622100652/http:/isasecurity.org/patternz].

so, it is not possible to know whether such an audit would be practical or effective. All that we can know is that this audit, whatever it may be, is not frequent:

> Google reserves the right to audit Buyer's use of the Real-time Bidder feature and investigate any related activity in order to ensure Buyer's compliance with these policies and the Authorized Buyers Terms. The audits shall be at Google's expense and will be conducted no more than once during each 12 month period, during normal business hours and without unreasonably interfering with Buyer's normal business operations.[56]

43. It is likely that an audit to uncover what has happened to billions of data points about Americans is impossible. In any case, Google appears to rely on investigative reporters to determine when to stop sending data to a company: it only stopped sharing RTB data with one company after several years when it was approached by a reporter in 2024.[57]

44. In 2024, Google appears to have introduced some form of identity verification for new customers of its RTB system.[58] At that time or before, Google may also have begun to send what it calls "non-personalized" bid requests when it understands the customer is controlled by a foreign adversary country. It should be noted that while Google's so-called "non-personalized" bid requests remove or generalize some RTB bid request data, they contain many more, including granular timestamp, partial user agent, URL or app ID, segment ID, and so on. This remains sensitive personally identifiable data in the meaning of 15 U.S.C. § 9901(c)(5).[59]

Indirectly making data available

45. Not only does Google directly share RTB data with foreign adversary countries, it also releases RTB data at so vast a scale and without any protections that it makes it available indirectly to foreign adversary countries. It shares RTB data about United States individuals 31 billion times per day, according to data obtained from Google by Enforce in 2023.[60] Despite the enormous scale of this sharing of personally identifiable sensitive

[56] *Authorized Buyers Program Guidelines*, Google Authorized Buyers (Sept. 9, 2024), https://www.google.com/intl/en/authorizedbuyers/guidelines/.
[57] Joseph Cox, *Inside a Global Phone Spy Tool Monitoring Billions*, 404 Media, (Jan. 24, 2024), https://www.404media.co/inside-global-phone-spy-tool-patternz-nuviad-real-time-bidding/.
[58] *Authorize Buyers Program Guidelines*, Google Authorized Buyers (Sept. 9, 2024), https://www.google.com/intl/en/authorizedbuyers/guidelines/.
[59] *Non-Personalized Ad Requests*, Google Authorized Buyers Help, https://support.google.com/authorizedbuyers/answer/11121285.
[60] Enforce Report, *supra* note 2, at 7.

data of United States individuals, Google releases the data without adequate safeguards to protect it.

46. After a DSP (or any other company) has received a bid request from Google, there is no way of controlling what it subsequently does with that data. Google's "Program Guidelines" forbid them from retaining and using this sensitive data about Americans.[61] But this is merely a statement on paper rather than a meaningful protection. In reality, the industry trade body states in public documentation that "publishers recognize there is no technical way to limit the way data is used after the data is received by a vendor for decisioning/bidding on/after delivery of an ad but need a way to clearly signal the restriction for permitted uses in an auditable way[.]"[62] Google has no way to avoid the data that it has broadcast from being shared on with foreign adversary countries.

47. Google's internal communications show that Google has known that its RTB system is a security risk since at least as early as 2014.[63] A senior Google executive asked, "[d]o we have any knowledge of whether bidders are reselling their data?" The resulting discussion concluded with an acknowledgement that "[t]he difficulty in figuring out what buyers are actually doing with data we're sending makes this tough." Auditing what parties that receive RTB data from Google is "tough because we mostly send data, not ingest."

48. An internal Google planning document from late 2021 noted the objective "Make RTB privacy safe" over the next three years.[64] The document indicates this would be achieved by switching off third-party cookies. Whether or not such a step would have been effective, Google did not follow through to switch off third-party cookies. In fact, it has done the opposite.[65]

49. Enforce's investigation also uncovered a list of Google RTB "segment data" that are available for purchase on the commercial market from a data broker other than Google. Purchasing a segment allows any buyer (perhaps acting through intermediaries) to target people within the segment by using Google's RTB system, thereby singling them out. The table below provides a sample of the sensitive national security examples from

---

[61] *Authorized Buyers Program Guidelines*, Google (last updated Sept. 9, 2024), https://www.google.com/intl/en/authorizedbuyers/guidelines/.
[62] *pubvendors.json v1.0: Transparency & Consent Framework*, IAB TechLab (Apr. 25, 2019), https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/pubvendors.json%20v1.0%20Draft%20for%20Public%20Comment.md.
[63] Plaintiffs' Exhibit PTX0326 Google Document (Mar. 31, 2016), *United States et al v. Google LLC*, 1:23-cv-00108, (E.D. Va. 2023), available at https://www.justice.gov/atr/media/1369416/dl?inline.
[64] Plaintiffs' Exhibit PTX1069 2022 AViD Sellside Plan, *United States et al v. Google LLC*, 1:23-cv-00108, (E.D. Va. 2023), GOOG-AT-MDL-008885748, available at https://storage.courtlistener.com/recap/gov.uscourts.vaed.533508/gov.uscourts.vaed.533508.1248.2.pdf.
[65] *See* Commentary, @thezedwards.bsky.social, Bluesky (Nov. 12, 2024, 8:50 PM), https://bsky.app/profile/thezedwards.bsky.social/post/3las7onxnds2o.

among the 25,854 Google RTB segments, including national security "decision makers," military logistics, active military, and judges:

Table: Examples of Google RTB Sensitive Data about United States National Security, Defense Industry, and Armed Forces Personnel

Segment name	**Description of segment**	**Google segment ID**
"Eyeota - B2B - Decision Makers - Government Industry - National Security and International Affairs"	"Users who are decision makers for the Government Industry, specifically National Security and International Affairs"	790212316
"Global Bombora - B2B - Industry - Manufacturing - Aerospace and Defense"	"People who work at companies in aerospace manufacturing."	27271699
"Global Fifty - Business & Industrial - Transportation & Logistics (B2B) - Aerospace & Defense"	"Business & Industrial > Transportation & Logistics (B2B) > Aerospace & Defense B2B Interest type segment"	6985997321
"US Selling Simplified - Job Function - Military and Protective Services - Seniority – Senior"	"Individuals whose Job Function is Military and Protective Services and Seniority is Senior"	808970298
"US Peoplefinders DaaS - B2B - Professional Groups - Criminal Justice Professionals – Judges"	"People who are likely Judges"	735904828
"US Adstra - Political - Social Profiles by Type - Active Military"	"Individuals who are active military. or an individual with a military address"	6978667300, 8053424913

50. The second table below of data segments uncovered by the Enforce investigation provides a sample of segments that correspond to categories (B), (C), (I), (L), (M), (N), (O), and (P) of the PADFAA definition of sensitive data at 15 U.S.C. § 9901(c)(7). Separately, Google's sharing and release of category (F) is evident from Google's documentation cited in the section above.

Table: Examples of Google RTB Sensitive Data about United States Individuals That are Commercially Available

§ 9901(c)(7) Sensitive data definition	Segment name	Description of segment	Google segment ID
(B) Any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or healthcare condition or treatment of an individual.	"US Adstra - Health - Disease Propensity by Type/Rx Use - Atrial Fibrillation Propensity"	"Individuals likely to have a Cardiovascular condition, such as Atrial Fibrillation, that is treated with a Prescription/Rx medication."	7238227915
(C) A financial account number, debit card number, credit card number, or information that describes or reveals the income level or bank account balances of an individual.	"US PowerB2B by MeritB2B - Estimated Income Personal - $500,000-749,999"	"This segments targets Decision Makers, Business Professionals and Individuals estimated income range (personal) - $500,000-749,999"	6861230196
(I) Information identifying the sexual behavior of an individual.	"US Kantar - Demographics - LGBT - Lesbian gay homosexual"	"Audiences who identify themselves as Lesbian, gay, or homosexual. Source: survey data from the MARS Consumer Health Study."	8052254759
(L) Information revealing the video content requested or selected by an individual.	"US TiVo - FOX News Channel Viewers"	"Viewers of FOX News Channel within the broadcast quarter. Seeded by TiVo 1st party deterministic data, modeled to represent national footprint."	7338842091
(M) Information about an individual under the age of 17.	"Eyeota - Demo - Education - Student - High School"	"Users who are currently High School Students"	790213993
(N) An individual's race, color, ethnicity, or religion.	"US Experian - Ethnic Insight -	"This segment contains consumers who are identified to have Hispanic ethnicity based on	458654602

	Ethnic Group – Hispanic"	sophisticated geocentric research and proprietary technology."	
(O) Information identifying an individual's online activities over time and across websites or online services.	"Global Ziff Davis - Ziff Davis - Interests - Technology - Business (B2B) – Security"	"Users likely responsible for enterprise systems security, based on users searching, browsing, downloading whitepapers, and/or subscribing to content related to security solutions"	876777748
(P) Information that reveals the status of an individual as a member of the Armed Forces.	"US Peoplefinders DaaS - Government - Politics - Military – Airforce"	"People who are in the Airforce Military Branch"	735905719

51. Google RTB segments discovered by Enforce reveal Americans who are gun owners. For example, Google segment ID 395090981 identifies "likely gun owners" provided by a data broker called Stirista. Google segment ID 772330995 from data broker Alliant identifies "the top 10% of households that hunt with rifle, shotgun, bow & arrow etc."[66] Congressman Warren Davidson's letter to Speaker Johnson and Majority Leader Scalise shows the concern among House Republicans about the trade in such data.[67]

52. These data are collected by other data brokers from diverse sources, likely including RTB, and are then shared and released by Google's RTB system for targeting using RTB. Segments are provided with RTB segment identification codes so that people they categorize can be identified by other entities via the RTB system.

53. Similarly, in November 2024, reporters revealed that they were able to buy data about the movements of U.S. intelligence and military personnel that had been collected using RTB. They discovered that "anyone can buy data tracking US soldiers and spies to nuclear vaults and brothels in Germany[.]"[68] Even people at sensitive U.S. intelligence facilities were unaware that "the device they're carrying with them everywhere is putting

[66] *See* "Doc 3" cited in Enforce Report, *supra* note 2, at 4.
[67] Warren Davidson Letter to Mike Johnson & Steve Scalise (Feb. 2024), https://www.politico.com/f/?id=0000018d-9edd-d7fe-abbd-deff0e8f0000.
[68] Dhruv Mehrotra & Dell Cameron, *Anyone Can Buy Data Tracking US Soldiers and Spies to Nuclear Vaults and Brothels in Germany*, Wired (Nov. 19, 2024), https://www.wired.com/story/phone-data-us-soldiers-spies-nuclear-germany/.

US national security at risk."[69] This realization is not new. Several years earlier, RTB revealed the movements of individual U.S. military special operators in Syria and Kuwait, and at Fort Bragg and Fort Hood.[70] The reporter confirmed that much of the data was from RTB when queried by Enforce.

54. Google's irresponsible and dangerous behavior since at least as early as 2014 is a choice. This is apparent because in addition to its normal RTB system, Google offers an alternative form of RTB called "non personalized ads" that shares much less data,[71] though enough to be dangerous. The choice to persist with standard RTB comes from Google's CEO himself. In January 2021 Google's Chief Marketing Officer wrote to CEO Sundar Pichai urging him to take a new approach:

> Be more focused about which parts of the ads business we want to get behind (i.e. real time bidding on user data = bad; contextual ads in search = good).[72]

55. Sundar Pichai chose to not do so. Instead, Google allows its customers to receive personally identifiable sensitive data about United States individuals and build dossiers about them. For example, Google's technical documentation shows customers how to use Google's "joinable fields" to stitch together information about individuals.[73] The data is the product.

56. Google does not appear to have taken any material or effective step to limit the data it shares. Indeed, it plans to do the opposite next month: in February Google will apply a new policy that it says is "less prescriptive with partners in how they target and measure ads."[74] The new policy removes restrictions on the use of IP addresses and "user agent"

---

[69] Dhruv Mehrotra & Dell Cameron, *Anyone Can Buy Data Tracking US Soldiers and Spies to Nuclear Vaults and Brothels in Germany*, Wired (Nov. 19, 2024), https://www.wired.com/story/phone-data-us-soldiers-spies-nuclear-germany/.

[70] Byron Tau, *The Ease of Tracking Mobile Phones of U.S. Soldiers in Hot Spots,* Wall Street Journal (Apr. 26, 2021) https://www.wsj.com/articles/the-ease-of-tracking-mobile-phones-of-u-s-soldiers-in-hot-spots-11619429402.

[71] *Non-Personalized Ad Requests,* Google Authorized Buyers Help, https://support.google.com/authorizedbuyers/answer/11121285.

[72] Email from Lorraine Twohill to Sundar Pichai, et al., *United States, et al., v. Google*, 1:20-cv-03010 (D.D.C.), dated Jan. 29, 2021, available at https://www.justice.gov/d9/2023-11/417790.pdf.

[73] *Joinable Fields in Ads Data Hub*, Google Ads Data Hub, https://developers.google.com/ads-data-hub/reference/field-joins.

[74] *Upcoming February update to the platforms program policies*, Google Platform Policies Help (Dec. 18, 2024), https://support.google.com/platformspolicy/answer/15610408?sjid=9639521737677950377-EU#022025.

data to single out a specific person's device.[75] The UK Information Commissioner's Office publicly stated this change is an "irresponsible" act by Google.[76]

57. The Dutch Government's 2024 annual cybersecurity assessment noted that "state actors can also be part of data trade through front companies" and highlighted RTB as a national security threat.[77]

D. Regulators and Lawmakers Have Raised Concerns About the Privacy and National Security Hazards of Real-Time Bidding

58. Following GDPR complaints,[78] European data protection authorities made a joint decision at the European Data Protection Board (EDPB) in February 2022. The Decision, which concerned a consent system that Google and other RTB participants rely on, makes the following findings of fact about RTB:[79]

> Real-time bidding poses a number of risks that stem from the nature of the ecosystem and the way personal data is processed within it. These risks include:
>
> - profiling and automated decision-making;
> - large-scale processing (including special categories of personal data);
> - innovative use or application of new technological or organizational solutions;
> - matching or merging of datasets;
> - analysis or prediction of behavior, location or movements of natural persons;

---

[75] *See* New Policy At Overview Of The Platforms Programs Policies Update (February 2025), Google Platform Policies Help, (Dec. 18, 2024), https://support.google.com/platformspolicy/answer/15738904; *See* previous policy at *Platforms Program Policies*, Google Platforms Policies Help (last updated Feb. 28, 2024), https://support.google.com/platformspolicy/answer/3013851?visit_id=638717543237329296-2004533841&hl=en&rd=1.

[76] Stephen Almond, *Our Response to Google's Policy Change on Fingerprinting*, UK Information Commissioner's Office (Dec. 19, 2024), https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/12/our-response-to-google-s-policy-change-on-fingerprinting/.

[77] *Cybersecurity Assessment Netherlands 2024*, National Coordinator for Counterterrorism and Security at 39 (Oct. 28, 2024), https://english.nctv.nl/documents/publications/2024/10/28/cybersecurity-assessment-netherlands-2024.

[78] *See* Lead Complaint and Chronology, *RTB Online Ad Auctions*, Enforce (2024), https://www.iccl.ie/rtb/#chronology.

[79] Article 60 Final Decision of February 2022, Case number: DOS-2019-01377, Litigation Chamber of the Data Protection Authority (Feb. 2, 2022), https://www.edpb.europa.eu/system/files/2022-03/be_2022-02_decisionpublic_0.pdf.

- invisible processing of personal data.

> In addition, a large number of organizations — such as data controllers, joint data controllers, processors or other data subjects — are part of the ecosystem. This has a potentially significant impact on data protection. Moreover, most data subjects have a limited understanding of how the ecosystem processes their personal data.
>
> As a result, the GDPR applies to the processing operations carried out within the framework of RTB, which are of such a nature that they can create a significant risk to the rights and freedoms of individuals.

59. The EDPB Decision states that RTB poses great risks, explaining that the architecture of OpenRTB supports:[80]

> [A] system posing great risks to the fundamental rights and freedoms of the data subjects, in particular in view of the large scale of personal data involved, the profiling activities, the prediction of behaviour, and the ensuing surveillance of data subjects.

60. In July 2020, ten members of Congress, led by Senators Cassidy and Wyden, wrote a bipartisan letter to then FTC Chairman Joseph Simons urging the Commission to investigate privacy violations resulting from RTB and to hold companies accountable under Section 5 of the FTC Act.[81]

61. In April 2021, Senators Cassidy, Wyden, Gillibrand, Warner, Brown and Warren sent letters to seven advertising exchanges, including Google, and requested they name the foreign firms they have provided U.S. RTB data to.[82] One SSP, Magnite, provided a list of 150 companies, several of which were based in China and Russia.[83]

---

[80] *Id.*, at para. 535.

[81] Letter from Sen. Ron Wyden, et al. to Joseph J. Simons, Federal Trade Commission Chair (Jul. 31, 2020), https://www.wyden.senate.gov/imo/media/doc/073120%20Wyden%20Cassidy%20Led%20FTC%20Investigation%20letter.pdf.

[82] *Wyden, Bipartisan Senators, Question Online Ad Exchanges on Sharing of Americans' Data with Foreign Companies*, Press Release (Apr. 2, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-bipartisan-senators-question-online-ad-exchanges-on-sharing-of-americans-data-with-foreign-companies (letter available at https://www.wyden.senate.gov/download/040121-wyden-led-bidstream-letter-to-att).

[83] Joseph Cox, *The Hundreds of Little-Known Firms Getting Data on Americans*, Vice (June 28, 2021), https://www.vice.com/en/article/hundreds-companies-bidstream-data-location-browsing/.

62. In August 2020, FCC Commissioner Geoffrey Starks launched an inquiry into AT&T and Verizon to investigate how each company broadcasts individuals' RTB location data.[84]

63. In August 2022, the FTC brought a lawsuit against Kochava for, among other things, providing location and mobile advertising ID data to track Americas in the advertising system.[85]

64. In December 2024, the FTC found that Mobilewalla had violated Section 5(a) of the FTC Act, 15 U.S.C. §45(a), which prohibits "unfair or deceptive acts or practices in or affecting commerce." Mobilewalla told the FTC it collected data on more than 2 billion people ("unique advertising identifiers") in the year and a half between January 2018 and June 2020, 60% of which came from RTB exchanges.[86]

65. The FTC's 2024 complaint against Mobilewalla summarizes the hazard that RTB causes Americans:[87]

> Mobilewalla has created a vast repository of consumer location information that enables Mobilewalla and its clients to track consumers' movements and, by virtue of knowing where the consumers traveled, to infer other sensitive information about consumers over years. Such vast amounts of data about identifiable individual consumers makes them vulnerable to significant harms, including stalking, targeted scams, and a variety of reputational harms.
>
> For example, using Mobilewalla's data, a client proposed to geo-fence the homes of individuals relevant to a private lawsuit and track where those individuals had traveled over the preceding two years, including whether they visited federal law enforcement offices. Additionally, Mobilewalla has marketed its ability to determine whether a consumer attended any political rallies in the last five years. Respondent has even begun to collect and store indefinitely clear text phone numbers and hashed phone numbers and email addresses, paired with MAIDs, which could be used to identify the name of the consumer associated with the sensitive location data.

---

[84] *Commissioner Starks Seeks Details On "Bidstream" Consumer Data And Procedures To Ensure Data Privacy*, FCC Press Release (Aug. 5, 2020), https://docs.fcc.gov/public/attachments/DOC-365979A1.pdf.
[85] Complaint for Permanent Injunction and Other Relief, *Fed. Trade Comm'n. v. Kochava*, 2:22-cv-00377 (D. Idaho), https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf.
[86] Complaint, *In re Mobilewalla*, Fed. Trade Comm'n No. 202-3196 at paras. 11 and 14. https://www.ftc.gov/system/files/ftc_gov/pdf/2023196mobilewallacomplaint.pdf.
[87] Complaint, *In re Mobilewalla*, Fed. Trade Comm'n No. 202-3196 at paras. 49 and 50, https://www.ftc.gov/system/files/ftc_gov/pdf/2023196mobilewallacomplaint.pdf.

66. The majority Commissioners referred to the Enforce 2023 report on RTB data in their statement about the FTC's action against Mobilewalla, highlighting the profound national security implications:[88]

> Last year a new report revealed the relative ease with which foreign adversaries can gather sensitive data on Americans. Foreign states could identify, for example, whether someone has a substance abuse problem, a gambling addiction, or major financial problems—a "torrent of blackmail data" ripe for abuse. The report noted that people susceptible to this type of surveillance include active military personnel, defense officials, lawmakers, and judges.

IV. Legal Analysis

A. Protecting Americans Data from Foreign Adversaries Act (PADFAA)

67. The Protecting Americans Data from Foreign Adversaries Act (PADFAA) prohibits data brokers from transferring personally identifiable sensitive data of United States individuals to any foreign adversary country or any entity controlled by a foreign adversary:[89]

> It shall be unlawful for a data broker to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available personally identifiable sensitive data of a United States individual to—
>
> (1) any foreign adversary country; or
> (2) any entity that is controlled by a foreign adversary.

68. A "Foreign Adversary Country" is defined as in 10 U.S.C. § 4872(d)(2): Democratic People's Republic of North Korea, People's Republic of China, Russian Federation, and Islamic Republic of Iran.[90]

69. PADFAA defines "[p]ersonally identifiable sensitive data" as any sensitive data that identifies or is linked or reasonably linkable, alone or in combination with other data, to

[88] Statement of Chair Lina M. Khan joined by Commissioner Alvaro M. Bedoya & Commissioner Rebecca Kelly Slaughter, *In re Mobilewalla, Inc.*, Fed. Trade Comm'n (Dec. 3, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/statement-khan-bedoya-slaughter-mobilewalla.pdf.
[89] PADFAA, 15 U.S.C. § 9901(a).
[90] PADFAA, 15 U.S.C. § 9901(c)(4).

an individual or a device that identifies or is linked or reasonably linked to an individual.[91]

70. At 15 U.S.C. § 9901(c)(7), PADFAA defines "[s]ensitive data" to include the following:[92]

> (B) "Any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or healthcare condition or treatment of an individual."
>
> (C) "…information that describes or reveals the income level or bank account balances of an individual."
>
> (I) "Information identifying the sexual behavior of an individual."
>
> (L) "Information revealing the video content requested or selected by an individual."
>
> (K) "Information about an individual under the age of 17."
>
> (N) "An individual's race, color, ethnicity, or religion."
>
> (O) "Information identifying an individual's online activities over time and across websites or online services."
>
> (P) "Information that reveals the status of an individual as a member of the Armed Forces."

71. 15 U.S.C. § 9901(c)(6) defines "precise geolocation information" as being "derived from a device or technology of an individual" and revealing the following:[93]

> past or present physical location of an individual or device that identifies or is linked or reasonably linkable to 1 or more individuals, with sufficient precision to identify street level location information of an individual or device or the location of an individual or device within a range of 1,850 feet or less.

[91] PADFAA, 15 U.S.C. § 9901(c)(5).
[92] PADFAA, 15 U.S.C. § 9901(c)(7).
[93] PADFAA, 15 U.S.C. § 9901(c)(6).

72. Any violation of PADFAA is treated as a violation of a rule defining an unfair or deceptive act or practice under Section 5 of the FTC Act.[94]

73. "Data broker" is defined as:[95]

> [A]n entity that, for valuable consideration, sells, licenses, rents, trades, transfers, releases, discloses, provides access to, or otherwise makes available data of United States individuals that the entity did not collect directly from such individuals to another entity that is not acting as a service provider.

B. FTC Act

74. Section 5 of the FTC Act prohibits unfair and deceptive acts and practices.[96]

75. A trade practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition."[97]

76. A deceptive trade practice is a material representation or omission that likely misleads a reasonable consumer. Deception occurs when a business makes a representation to consumers but "lacks a 'reasonable basis' to support the claims made."[98]

V. Google's Violations of PADFAA

A. Google is a Data Broker that Transfers Personally Identifiably Sensitive Data to Foreign Adversaries

77. As set forth above, Google's RTB system provides access to vast quantities of personally identifiable sensitive data of United States individuals that it did not collect directly to third parties. It is a system in which companies pay to access RTB data.

78. PADFAA provides an exception at 15 U.S.C. § 9901(c)(3)(B)(ii) for entities that offer "a product or service with respect to which personally identifiable sensitive data, or access to such data, is not the product or service[.]" This does not apply to Google's RTB.

---

[94] PADFAA, 15 U.S.C. § 9901(b)(1).
[95] PADFAA, 15 U.S.C. § 9901(b)(3).
[96] 15 U.S.C. § 45.
[97] *Policy Statement on Unfairness*, Fed. Trade Comm'n. (Dec. 17, 1980), https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness.
[98] *Policy Statement on Deception*, Fed. Trade Comm'n. (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

Google may claim it merely sells advertising "impressions" or "inventory" without brokering such data, but in fact it provides data as a service as shown in section III(C), above. As bipartisan senators themselves have noted, many entities participate in RTB auctions without any intention of ever placing an advertisement.[99] Privacy experts are in no doubt that Google operates as a data broker.[100] If Google claims that users' personal information is not its product or service, it should prove that to the Commission.

79. Nor do any other exclusions in 15 U.S.C. § 9901(c)(3)(B) apply to Google's RTB. It indirectly collects data from United States individuals when they use other companies' websites and apps, and from advertisers. This is true irrespective of whether Google can at other times directly collect data about individuals when they use Google's own websites and apps.

80. Google's RTB shares personally identifiable sensitive data of United States individuals with its RTB customers and partners (such as DSPs), which are not service providers in the meaning of 15 U.S.C. § 9901(c)(8).

81. Google provides access to sensitive data of United States individuals to foreign adversaries, sharing it directly, and making it available by releasing it at massive scale and without protections so that it indirectly is made available to foreign adversaries.

82. PADFAA was specifically passed to prevent the privacy and security risks associated with surveillance by foreign adversaries. Thus, for the foregoing reasons, Google's RTB practices are a significant enough risk of violating PADFAA and warrant urgent FTC investigation.

VI. Google's Violations of the FTC Act

[99] Letter from Sen. Ron Wyden, et al. to Joseph J. Simons, Federal Trade Commission Chair (Jul. 31, 2020), https://www.wyden.senate.gov/imo/media/doc/073120%20Wyden%20Cassidy%20Led%20FTC%20Investigation%20letter.pdf.

[100] "Sites like Facebook and Google now serve as de facto data brokers, aggregating data on users for the purpose of implementing powerful advertising platforms." Giridhari Venkatadri *et al.*, *Privacy Risks with Facebook's PII-Based Targeting: Auditing a Data Broker's Advertising Interface*, 2018 IEEE Symposium on Security and Privacy, https://www.ftc.gov/system/files/documents/public_events/1223263/p155407privacyconmislove_1.pdf (May 2018); Chris Hoofnagle, *Facebook and Google Are the New Data Brokers*, Cornell Tech (Jan. 5, 2021), https://www.dli.tech.cornell.edu/post/facebook-and-google-are-the-new-data-brokers; Bennett Cyphers, *Google Says It Doesn't 'Sell' Your Data. Here's How the Company Shares, Monetizes, and Exploits It.*, EFF (Mar. 19, 2020), https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and.

A. Google Unfairly Shares with and Makes Available Personally Identifiable Sensitive Data of United States Individuals to Foreign Adversary Countries

83. Google shares with and releases RTB data that include subsections (B), (C), (I), (K), (L), (N), (O), and (P) of the definition of sensitive data at 15 U.S.C. § 9901(c)(7) to foreign adversary countries.

84. The vast quantities of sensitive data that Google directly shares, and releases in a manner that makes it available indirectly, create substantial privacy and security harms for all consumers and expose United States national security personnel and their institutions to blackmail and hacking. Military personnel and people working in sensitive industries (e.g., aerospace & defense, nuclear energy) are particularly vulnerable.[101]

85. This injury is not reasonably avoidable by consumers themselves because Google is not transparent about its RTB process and does not give consumers the option to opt out of their data being used in auctions altogether.

86. Google's practice of broadcasting sensitive personal information during the RTB process is not outweighed by any countervailing benefits to competition or consumers. Google's collection and maintenance of personal information—the valuable product in the RTB ecosystem—is anticompetitive. This maintains Google's market dominance. Further, there are no countervailing benefits to consumers[102] when their personal information is leaked to foreign adversaries, exposing them to exploitation, manipulation, and blackmail.

B. Google's Deceptive Transfer of Sensitive Data

87. Google promises consumers that it will not "sell" their sensitive user data unless they consent. Google fails to also say that it broadcasts their sensitive personal information widely for profit, and cannot control where that data ends up, allowing other entities—including foreign adversaries—to access users' sensitive information.

88. There is no conspicuous mechanism for consumers to opt out of their data being used for RTB auctions or to request that Google not share one's information with a foreign adversary. Nor does Google provide a right to opt out of all information sharing.

---

[101] ICCL Enforce Report, *supra* note 2, at 11–13.

[102] *See Unfair & Deceitful Commercial Surveillance Submission to the United States Federal Trade Commission*, ICCL Enforce and Open Markets Institute and Trans Atlantic Consumer Dialogue at 10–15 (Nov. 2022), https://www.iccl.ie/wp-content/uploads/2022/11/ICCL-Open-Markets-TACD-comment-on-FTC-call-commercial-surveilance-rulemaking.pdf.

89. For example, on January 7, 2025 the United States District Court for the Northern California observed about Google's "Activity Controls" and "Web & App Activity" controls that:

> On the <Activity Controls> page and connected interfaces, which include the WAA and (s)WAA settings and their descriptions, Google provides multiple descriptions of what the WAA and (s)WAA settings entail. Nowhere do these disclosures indicate with reasonable clarity that (s)WAA controls not whether Google will collect data about a user's app activity at all, but only whether Google will delink the collected data from the user's GAIA-ID. The various interpretations of these disclosures render them ambiguous such that a reasonable user would expect the WAA and (s)WAA settings to control Google's collection of a user's web app and activity on products using Google's services. Documents Google produced in discovery only emphasize the WAA settings' ambiguity.[103]

90. Google's material misrepresentations would likely mislead the ordinary consumer because no reasonable consumer would read Google's statements and understand them to mean that Google would allow their data to be accessed by foreign adversaries.

VII. Prayer for Relief

91. In view of enormous scale of the data sharing and the sensitivity of the data, we urge the Federal Trade Commission to investigate if Google, through its RTB practices, has violated the Protecting Americans Data from Foreign Adversaries Act and the FTC Act's prohibition of unfair and deceptive practices. At a minimum, we suggest that the Commission investigate to what extent Google engages in the following practices:

    a. Transfer of United States individuals' personally identifiable sensitive data to foreign adversaries at large scale;

    b. Google's failure to protect data it collects and shares in the RTB ecosystem;

    c. Google's vetting process for its third-party affiliates that may access or share consumers' information in the RTB process.

92. We further urge the Commission to:

[103] Order Denying Google's Motion For Summary Judgment, *Rodriguez et al. v Google, LLC*, 20-cv-04688 (N.D. Cal. 2024), https://storage.courtlistener.com/recap/gov.uscourts.cand.362381/gov.uscourts.cand.362381.445.0.pdf.

a. Impose appropriate civil penalties pursuant to 15 U.S.C. § 45(1); and

b. Halt any sharing by Google of personally identifiable sensitive data of United States individuals with foreign adversaries. Google and IAB TechLab, whose technical specifications Google has adopted, should be required to amend the RTB systems so that no personally identifiable sensitive data are permitted in future RTB broadcasts. To do this, the FTC should require that all identifying and linkable data fields be removed from the "OpenRTB protocol" and from Google's implementation of that protocol. This includes removing high resolution timestamps, data extensions, unique identifiers, etc.

c. The above action can be enforced and monitored at SSPs and ad exchanges, of which Google is the largest one, and we urge the FTC to monitor this on an ongoing basis by way of randomized samples of bid requests.

93. In addition, we suggest that the Commission take the following steps:

a. Halt any unfair, deceptive, or otherwise unlawful collection, disclosure, and retention of sensitive personal data for RTB, by Google;

b. Require Google to implement and maintain an effective data minimization, protection, and deletion program with meaningful FTC oversight;

c. Require that Google prove it complies with PADFAA, regularly provide the Commission with evidence of its continued compliance;

d. Provide such other relief as the Commission finds necessary and appropriate.

Sincerely,

/s/ John Davisson
EPIC Director of Litigation &
Senior Counsel

/s/ Sara Geoghegan
EPIC Senior Counsel

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW

Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)

/s/ Dr. Johnny Ryan
Enforce Director & Senior Fellow

ENFORCE
Irish Council for Civil Liberties (ICCL)
First Floor, Castleriver House
14-15 Parliament Street
Dublin 2, D02 FW60
+353-1-9121640 (tel)