William J. Edelman (SBN: 285177)
MILBERG, PLLC
227 West Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (771) 474-1121
Email: wedelman@milberg.com

Heather M. Lopez (SBN: 354022)
MILBERG, PLLC
280 S. Beverly Drive-Penthouse,
Beverly Hills, CA 90212
Telephone: (331) 240-3015
Email: hlopez@milberg.com
Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

BARBARA JENKINS, individually and on behalf of all others similarly situated,

Plaintiff,

v.

GOOGLE LLC, a Delaware limited liability company,

Defendant.

Case No.:

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL FOR:

1. **Violation of 18 U.S.C. § 2511;**
2. **Violation of Md. Code Ann., Cts. & Jud. Proc. § 10-402;**
3. **Invasion of Privacy – Intrusion Upon Seclusion**
4. **Invasion of Privacy – Publication of Private Facts**

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Barbara Jenkins ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint ("Complaint") against Defendant Google LLC ("Google" or "Defendant"), and alleges as follows based upon personal knowledge as to her own acts and experiences, and upon information and belief, including investigation by counsel, as to all other matters:

NATURE OF THE ACTION

1. Every day, millions of Americans use the internet to research their medical conditions, find resources related to private family matters such as mental health concerns, parenting, and religion, and browse other sensitive content.

2. Users reasonably expect that their online activities and identities will be protected and not secretly intercepted and disclosed to Chinese technology conglomerates who answer to a foreign government.

3. However, that is exactly what Google has done in violation of federal and state law.

4. Google operates the world's largest digital advertising ecosystem, generating approximately $307.4 billion in annual revenue, the substantial majority of which it derives from its online advertising business.

5. Through this vast advertising infrastructure, Google intercepts information about Americans' browsing activity and assigns persistent, digital identifiers that track individuals through websites, apps, and devices.

6. Google transmits personal information at massive scale and without meaningful notice or valid consent, to third-party advertising entities participating in its ecosystem, including entities owned by, controlled by, or subject to the jurisdiction of the People's Republic of China.

7. Google's conduct violates federal regulations and wiretapping laws as well as state statutes and laws.

8. The receiving entities include some of the most scrutinized Chinese technology companies in the world: MediaGo, a subsidiary of the Chinese search giant Baidu; Pangle, operated by ByteDance, the Chinese parent company of TikTok; and Temu, affiliated with PDD Holdings, a Chinese-owned entity.

9. Each of these companies are subject to Chinese laws that require cooperation with China's government intelligence operations. This constitutes a substantial risk and an ongoing cybersecurity concern because the Chinese government may already be accessing and actively using

private user data.[1]

10. In April 2025, the federal government implemented the Bulk Sensitive Data Rule ("BSDR"), which categorically prohibits the commercial transfer of Americans' bulk sensitive personal data, including IP addresses and persistent online identifiers, to entities subject to the jurisdiction of countries of concern, including China. The rule reflects the government's determination that such transfers pose an "unusual and extraordinary threat" to the national security of the United States.

11. Google's cookie syncing and real-time bidding operations violate the BSDR.

12. Google intercepts users' electronic communications for the purpose of making these unlawful transfers and violating Americans' privacy in violation of the Electronic Communications Privacy Act ("ECPA" or "Federal Wiretap Act"), 18 U.S.C. § 2511(2)(d), rendering Google liable to every American whose communications it intercepted and whose data it transmitted to covered foreign persons. Google's conduct independently violates Maryland's wiretapping statute Md. Code Ann., Cts. & Jud. Proc. § 10-402.

13. Through this action, Plaintiff seeks to hold Google accountable for operating the infrastructure through which Americans' sensitive online activity is transmitted to advertising entities subject to the jurisdiction of a designated foreign adversary. On behalf of a nationwide class and a Maryland subclass, Plaintiff seeks statutory and compensatory damages for millions of affected individuals.

PARTIES

14. Plaintiff Barbara Jenkins is a natural person and citizen of Maryland who resides in Baltimore, Maryland.

15. Defendant Google LLC is a limited liability company organized under the laws of Delaware, with its principal place of business at 1600 Amphitheatre Parkway, Mountain View, California 94043. Google is a wholly owned subsidiary of Alphabet Inc.

[1] The term "user" means individuals, including Plaintiff and Class Members, who used websites, apps, and/or devices on which Google's embedded software secretly intercepted communications and disclosed them to third-parties in violation of state and federal law.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2) because this is a class action in which the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and at least one member of the class is a citizen of a state different from the Defendant.

17. This Court also has federal question jurisdiction under 28 U.S.C. § 1331 because Plaintiff's claims arise under federal law, specifically the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq*.

18. This Court has supplemental jurisdiction over Plaintiff's state-law claims under 28 U.S.C. § 1367 because those claims arise from the same case or controversy as Plaintiff's federal claims under the ECPA.

19. This Court has personal jurisdiction over Defendant because Google is headquartered in this District, conducts substantial and continuous business within this District, and maintains its principal place of business at 1600 Amphitheatre Parkway, Mountain View, California, which is within this District. Google's advertising infrastructure, including the systems at issue in this action, is developed, maintained, and operated from facilities within this District.

20. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) and (b)(2) because Defendant resides in this District and because a substantial part of the events giving rise to Plaintiff's claims occurred in this District. Specifically, Google develops, maintains, and operates its advertising infrastructure, including the cookie syncing systems and real-time bidding platforms at issue, from its headquarters and facilities located within this District. The decisions to implement, configure, and maintain integrations with foreign advertising partners, including those subject to Chinese jurisdiction, were made and executed from within this District.

FACTUAL ALLEGATIONS

A. Overview of Online Advertising and Tracking Technologies

21. Online advertising is the primary revenue model for much of the internet. The value of a given advertisement depends on how precisely the advertiser can identify the person viewing it, their interests, demographics, and behavior across websites. For this reason, a sophisticated

ecosystem of tracking technologies has developed to identify and monitor users not just on a single website, but across many websites over time.

22. Two technologies are foundational to this ecosystem. The first is third-party trackers, typically a small piece of JavaScript code that website owners (also known as "publishers") incorporate into their website pages.[2] When a user loads a page containing that code, the tracker automatically and invisibly loads, generating background network requests to third-party advertising servers. Trackers can collect extensive information about a user's browsing activity, including the pages they visit, the search terms they enter, and the links they click. They can also collect technical information about the user's device and network connection.

23. The second is the HTTP cookie, which can function as a persistent identifier. A cookie is a small piece of data stored in the user's browser and tied to a particular web address (also known as a "domain", such as "doubleclick.net"). When the browser later sends a request to that same address, it automatically includes the cookie. In the advertising context, many websites load ads and trackers from the same advertising addresses across the internet (for example, Google's DoubleClick addresses). Because the browser contacts those same advertising addresses from site to site, the advertising company can recognize the same browser across multiple websites and browsing sessions and link those visits to a stable identifier.

24. Trackers and cookies work together. A tracker running in a user's browser can set new cookies, read existing cookies associated with the tracker's domain, and transmit both the cookie identifiers and the collected browsing data to third-party servers in a single request. The result is that when a user visits a website that embeds third-party advertising code, the advertising company simultaneously learns what the user is doing on that site and can link that activity to a persistent identifier that connects it to the same user's activity on other sites.

25. In recent years, many companies and systems have been moving away from the use of cookies, in part to provide the illusion of privacy and control. As a result, online advertisers, including Google, have invented new means of tracking individuals that rely on other persistent

[2] In addition to JavaScript codes, trackers may also be image pixels, iframes, SDK calls, etc., and this is especially true in mobile and server-side implementations.

identifiers such as mobile advertising identifiers ("MAIDs"), device identifiers, local storage, and other data points that allow for device fingerprinting.

26. This combination of real-time data collection and persistent identification across websites is the foundation of modern targeted advertising over which Google has been the primary architect.

B. Google's Tracking of Users Across the Internet

27. Google operates the world's largest online advertising network. Through products including Google Ads, Google Ad Manager, Google Publisher Tag, Google Ad Exchange, and the underlying DoubleClick infrastructure, Google's advertising code is embedded on a vast number of websites, likely millions, spanning virtually every category of online content. When a user visits any of these websites, Google's tracking scripts execute automatically in the user's browser, collecting information about the user's activity on that site and transmitting it to Google's servers at doubleclick.net and related domains.

28. As part of this process, Google sets and reads persistent cookies on users' browsers, including the IDE and DSID cookies. These cookies allow Google to recognize the same user across multiple websites and browsing sessions. The DSID cookie is directly linked to a user's Google account, meaning that Google can associate browsing activity collected across third-party websites with an identified individual if they are logged into their Google account (such as through Gmail or YouTube) in the same browser. The IDE cookie is a persistent cookie that is able to track and profile users even when they are not logged into a Google account. The result is that as a user moves across the internet, Google's tracking scripts and cookies work in tandem to build a detailed and personally identifiable profile of that user's browsing behavior over time.

29. Google's tracking scripts do not merely collect technical metadata. When a user visits a webpage, the URL of the user's request, including its full path and query parameters, reveals what page the user is seeking or what search terms they entered. The referrer, transmitted as part of the same request to the tracker, reveals the page the user came from. Together, these elements disclose what the user is looking for, what they are reading, and how they are navigating a website: the substance, purport, and meaning of the user's interaction with that site. Google's tracking code

acquires this information contemporaneously with the user's communication with the website, as the page loads and the user's interaction with the website is still underway, and transmits it to Google's servers alongside the user's persistent identifier cookies.

30. The user does not intend or direct any communication to Google. The user's browser sends a request to the website's server; Google's code, embedded in the website by the publisher, acquires the contents of that communication and transmits them to Google. The user has no direct relationship with Google's advertising infrastructure as deployed on third-party websites, receives no services from Google in connection with these transmissions, and has no meaningful opportunity to detect, review, or prevent Google's acquisition of their browsing activity.

C. Google's Transmission of User Data to Advertising Partners

31. Google does not merely collect user data for its own use. It shares that data with other advertising companies as part of the process of selling advertising space on the websites where its code is embedded. Google generates approximately $307.4 billion in annual revenue, the substantial majority of which derives from advertising.

32. The way this works is through automated auctions. Each time a user loads a webpage that uses Google's advertising tools, Google runs a real-time bidding ("RTB") auction to determine which advertisement to display. In a fraction of a second, Google sends out "bid requests" to solicit bids from advertising companies approved to participate in its ecosystem, then selects a winning bidder, before delivering that bidder's advertisement to the user. Google controls every stage of this process: it operates the auction, serves the ad, and determines which advertising companies are eligible to participate.

33. To enable bidders to decide how much to bid, Google provides the advertising companies with information about the user and the page being viewed. These bid requests include the URL of the page the user is viewing and referrer, the user's IP address, IP-derived geolocation, and cookie data.[3] According to Google's own technical documentation, bid requests may also include

[3] Google for Developers, *OpenRTB Integration,* https://developers.google.com/authorized-buyers/rtb/openrtb-guide (last accessed, Feb. 11, 2026); Google for Developers, *Geographical Targeting,* https://developers.google.com/authorized-buyers/rtb/geotargeting (last accessed, Feb. 11, 2026).

audience classification codes drawn from the IAB TechLab Audience Taxonomy, a standardized list of over 1,999 characteristics that can be assigned to individual users (including, for example, their involvement in aerospace and defense procurement or their use of payday and emergency loans),[4] as well as content classification codes drawn from the IAB TechLab Content Taxonomy, which categorize the subject matter of the page or app content the user is viewing and span sensitive categories including bankruptcy, mental health, substance abuse, sexual conditions, and specific religious traditions.[5]

34. As part of the RTB process, Google also conducts an ongoing "cookie syncing" process, which Google calls "cookie matching." This involves Google sharing an internal identifier known as the Google GID. Unlike the IDE and DSID cookies, the Google GID is not stored in the user's browser. It is a Google-assigned advertising identifier that Google embeds directly into communications with its advertising partners. Each advertising company assigns its own identifier to users, but one company cannot read another company's identifiers. Without cookie syncing, an advertising partner receiving a bid request from Google would have no way to connect Google's identifier for a user to the partner's own records for that same person. Cookie syncing solves this problem. Through the process, Google transmits the Google GID to the partner's endpoint, and the partner links it to its own identifier for the same user. Once this link is established, the partner can recognize the same user each time it receives a bid request from Google, look up what it already knows about that user, and bid accordingly.

35. The effect of Google's RTB and cookie syncing processes is that approved advertising partners receive the persistent GID advertising identifier, enabling them to recognize and track the

---

[4] *See* Google Authorized Buyers, *OpenRTB Integration,* https://developers.google.com/authorized-buyers/rtb/openrtb-guide#dataext; *linking to* InteractiveAdvertisingBureau, *Audience Taxonomy 1.1*, https://github.com/InteractiveAdvertisingBureau/Taxonomies/blob/main/Audience%20Taxonomies/Audience%20Taxonomy%201.1.tsv (last accessed, Feb. 12, 2026).

[5] *See* Google Authorized Buyers, *OpenRTB Integration*, https://developers.google.com/authorized-buyers/rtb/openrtb-guide#dataext; *linking to* InteractiveAdvertisingBureau, *Content Taxonomy 2.2*, https://github.com/InteractiveAdvertisingBureau/Taxonomies/blob/main/Content%20Taxonomies/Content%20Taxonomy%202.2.tsv (last accessed, Feb. 12, 2026).

same user over time, and, upon information and belief, the substance of the user's browsing activity through the URLs and other data included in bid requests. Google's advertising infrastructure thereby functions as a mechanism through which user data collected from third-party websites is transmitted to advertising partners that have no direct relationship with the user and that did not collect or process the data directly from the individuals to whom it relates.

36. Google's RTB process involves the sharing of users' IP addresses with its advertising partners. An IP address is a globally unique numerical identifier that routes communications across the internet. IP addresses reveal the geographic location of internet users; publicly available lookup services can map an IP address to a country, city, and approximate coordinates with over 95% accuracy. IP addresses are particularly powerful when combined with persistent identifiers like advertising cookies. As individuals use their devices across different locations, such as home, work, and elsewhere, each location has its own IP address. By tracking these movement patterns and correlating them with a persistent cookie or advertising identifier, an advertising company can build detailed profiles of individual users' daily routines and behaviors, distinguishing them from others who may share the same IP address.

37. The result is that Google's RTB infrastructure functions as a hub for identity propagation across the advertising ecosystem. Through its cookie syncing systems, Google enables each of its approved advertising partners to recognize the same user across Google-run auctions, link that user to the partner's own tracking systems, and build profiles informed by activity observed across unrelated websites. Google remains central not only to the execution of individual ad transactions but also to the creation, coordination, and sharing of user identifiers among the companies that participate in its ecosystem.

D. Google's Foreign and Chinese-Affiliated Advertising Partners

38. Among the advertising partners formally approved to participate in Google's RTB ecosystem and receive user data through the processes described above are multiple entities owned by, controlled by, or affiliated with companies headquartered in or subject to the jurisdiction of the

People's Republic of China.[6] Three are relevant here: Pangle, operated by ByteDance Pte. Ltd.; MediaGo, operated by Baidu USA LLC; and Temu, operated by Whaleco Services, LLC.

39. *Temu and PDD Holdings:* Temu is the global online marketplace brand operated in the United States by Whaleco, Inc., a wholly owned subsidiary of PDD Holdings Inc. PDD Holdings is the ultimate parent entity of Temu, which exercises strategic and economic control over its operations, and maintains substantial operations, personnel, and affiliated entities in the People's Republic of China. PDD Holdings is subject to Chinese law, including China's National Intelligence Law, Cybersecurity Law, and Data Security Law, which may require cooperation with state intelligence authorities. In 2024, twenty-one state attorneys general issued a formal warning about Temu's invasive data practices and its legal obligations under Chinese law.[7] In 2025, the attorneys general of Nebraska and Kentucky filed lawsuits against Temu, alleging that its mobile app functions as spyware.[8]

40. *ByteDance and Pangle:* ByteDance Ltd. is a Chinese technology company headquartered in the People's Republic of China and the parent company of TikTok. ByteDance's relationship with the Chinese state has been the subject of congressional investigation, executive action, and proposed federal legislation. As part of its advertising ecosystem, ByteDance owns and operates Pangle, an advertising network that facilitates ad monetization and distribution across

---

[6] Google publicly maintains partner and vendor lists for its major advertising products, including Google Ads and Google Ad Manager / Ad Exchange: Google for Developers, *Google Ads Certified External Vendors*, https://developers.google.com/third-party-ads/googleads-vendors (last accessed Feb. 11, 2026); Google for Developers, *Ad Manager Certified External Vendors*, https://developers.google.com/third-party-ads/adx-vendors (last accessed Feb. 11, 2026).

[7] Letter from Attorneys General of 21 States to Temu (WhaleCo Inc.) and PDD Holdings Inc. (Aug. 15, 2024), available at https://www.iowaattorneygeneral.gov/media/cms/Temu_Request_Letter_FINAL_BC5E1C51FF39A.pdf (last accessed, Feb. 11, 2026).

[8] Press Release, Nebraska Attorney General, *Attorney General Hilgers Files Lawsuit Against Temu for Siphoning Nebraskans' Phone Data* (June 12, 2025), https://ago.nebraska.gov/attorney-general-hilgers-files-lawsuit-against-temu-siphoning-nebraskans-phone-data (last accessed, Feb. 11, 2026); Press Release, Kentucky Attorney General, *Attorney General Coleman Files Lawsuit Against Chinese Shopping Platform Temu for Stealing Kentuckians' Data* (July 17, 2025), https://www.kentucky.gov/Pages/Activity-stream.aspx?n=AttorneyGeneral&prId=1797 (last accessed, Feb. 11, 2026).

TikTok and affiliated third-party mobile applications. Pangle is operated by ByteDance Pte. Ltd., a ByteDance subsidiary, and remains under ByteDance's ownership and control. ByteDance is subject to Chinese law, including China's National Intelligence Law, Cybersecurity Law, and Data Security Law, which can require cooperation with government intelligence operations and create a risk of government access to private user data.

41. *Baidu and MediaGo:* Baidu, Inc. is a Chinese technology company headquartered in Beijing and one of the largest internet companies in China. Through its advertising business, Baidu owns and operates MediaGo, a digital advertising platform run by its subsidiary Baidu USA LLC. MediaGo's own privacy policy expressly references its relationship to Baidu and the processing of information in connection with Baidu corporate operations.[9] Baidu is subject to the People's Republic of China's cybersecurity, data security, and related national security legal frameworks, which can require cooperation with government intelligence operations and create a risk of government access to private user data.

E. Google's Cookie Syncing with Chinese-Affiliated Entities on Sensitive Websites

42. The example websites described below reflect the ordinary operation of Google's advertising systems on websites containing sensitive user information. In each instance, the processes described occur automatically during and after page load, without any affirmative action by the user. Google's tracking code intercepts the contents of users' communications with these websites, including URLs containing sensitive search terms and page content, and transmits those contents to Google's servers alongside persistent identifier cookies linked to users' identities and IP addresses. Through the RTB auction process, Google transmits the user's Google GID to Chinese-affiliated advertising partners through its cookie syncing process, and, through its RTB bid requests, shares with those same partners the URL of the page being viewed, the user's IP address, and other identifying information. The result is that Google both intercepts the substance of Americans' sensitive browsing activity and transmits their persistent identifiers and personal data to advertising entities subject to the jurisdiction of the People's Republic of China.

[9] MediaGo, *Privacy Policy* (last revised Nov. 11, 2025), https://cdn.mediago.io/js/officialWebsite/privacy.html (last accessed, Feb. 11, 2026).

43. *Drugs.com.* Drugs.com is a health information website that provides drug interaction tools, medication guides, and information about prescription drugs and medical conditions. User visits to the site may reveal sensitive information about an individual's health conditions, medications, and treatment decisions. When a user browse Drugs.com, Google's tracking code intercepts the substance of their browsing activity, including search terms entered and pages viewed, and transmits it to Google's DoubleClick infrastructure alongside the user's identifying cookies, IP address, and device information. For example, a search for "lithium" or a visit to an article on opioid safety transmits those terms within the URLs to Google in the same manner as any other user interaction with the site. As part of the RTB process on Drugs.com, Google transmits the user's Google GID to MediaGo (identified internally in Google's systems as baidu_mediago), Pangle (identified internally as toutiao_usd), and Temu (identified internally as whaleco_services_llc), and shares with these partners the URL of the page the user is viewing (which includes sensitive medical search terms and the names of the pages viewed), the user's IP address, IP-derived geolocation, and cookie data.

44. *BibleHub.com.* BibleHub.com is an online biblical reference resource offering searchable access to multiple Bible translations, concordances, commentaries, and cross-references. User visits to the site may reveal sensitive information about an individual's religious beliefs, moral reflections, and areas of spiritual struggle or discernment. When a user browse BibleHub.com, Google's tracking code intercepts the substance of their browsing activity, including search terms entered and pages viewed, and transmits it to Google's DoubleClick infrastructure alongside the user's identifying cookies, IP address, and device information. For example, a search for "temptation" or "adultery," or a visit to a specific Bible verse, transmits those terms within the URLs to Google in the same manner as any other user interaction with the site. As part of the RTB process on BibleHub.com, Google transmits the user's Google GID to Temu (identified internally as whaleco_services_llc) and Pangle (identified internally as toutiao_usd), and shares with these partners the URL of the page the user is viewing (which includes sensitive religious search terms and the specific biblical content being accessed), the user's IP address, IP-derived geolocation, and cookie data.

45. *Parents.com.* Parents.com is a parenting and family-focused website publishing articles and advice on pregnancy, child development, health, and family life. User visits to the site may reveal sensitive information about an individual's family structure, their children's ages and health, and their concerns as a parent. When users browse Parents.com, Google's tracking code intercepts the substance of their browsing activity, including articles viewed and topics explored, and transmits it to Google's DoubleClick infrastructure alongside the user's identifying cookies, IP address, and device information. For example, a visit to an article on childhood behavioral disorders or newborn health concerns transmits the names of these pages within the URLs to Google in the same manner as any other user interaction with the site. As part of the RTB process on Parents.com, Google transmits the user's Google GID to Temu (identified internally as whaleco_services_llc) and Pangle (identified internally as toutiao_usd), and shares with these partners the URL of the page the user is viewing (which includes sensitive parenting-related content being accessed), the user's IP address, IP-derived geolocation, and cookie data.

46. These examples are illustrative, not exhaustive. Google's advertising and cookie syncing infrastructure is deployed across a vast number of websites spanning sensitive categories including health, religion, parenting, finance, and many others. In each instance, Google intercepts the contents of users' communications with these websites and transmits their persistent identifiers and personal data to Chinese-affiliated advertising partners without any meaningful notice to or consent from the user.

F. The Bulk Sensitive Data Rule

i. History and Purpose

47. The Bulk Sensitive Data Rule ("BSDR") originates in Executive Order 14117, in which the President determined that the transfer of Americans' bulk sensitive personal data to countries of concern, including the People's Republic of China, presents a national security risk. The Executive Order reflects a shift in federal national security policy that recognizes foreign adversaries can obtain sensitive information about U.S. persons through ordinary commercial data flows, not only through cyber intrusions or traditional espionage.

48. The Department of Justice implemented Executive Order 14117 through the Data

Security Program, administered by the National Security Division and codified at 28 C.F.R. Part 202. DOJ has explained that the program is intended to prevent countries of concern from gaining access to Americans' bulk sensitive personal data through common commercial practices, including data brokerage, advertising technology, and cross-border data sharing. As a senior Justice Department official explained, the BSDR aims to stop foreign governments from sidestepping American cybersecurity protections entirely: "[W]hy would you go through the trouble of complicated cyber intrusions and theft to get Americans' data when you can just buy it on the open market or force a company under your jurisdiction to give you access? . . . The [BSDR program] makes getting that data a lot harder."[10]

ii. Structure of the BSDR

49. At a high level, the BSDR prohibits "covered data transactions," defined as transactions that involve the transfer of bulk sensitive personal data to a "covered person" through specified transaction types, including "data brokerage." See 28 C.F.R. §§ 202.210, 202.301(a). Whether a given transfer is prohibited turns on what data is being transferred, to whom, in what volume, and through what type of transaction.

50. *Sensitive Personal Data and Covered Personal Identifiers.* The BSDR defines a set of "listed identifiers" that includes, among other items, device identifiers, IP addresses, and cookie data. *See* 28 C.F.R. § 202.234(g). A listed identifier becomes a "covered personal identifier," and therefore "sensitive personal data" regulated by the BSDR, when it is transferred in combination with any other listed identifier, or in combination with other data such that it is linked or linkable to other listed identifiers or to other sensitive personal data. *See* 28 C.F.R. §§ 202.212(a), 202.249(a).

51. *Bulk Thresholds.* The BSDR's prohibitions apply when sensitive personal data is transferred in "bulk." For covered personal identifiers, the rule defines bulk as data relating to 100,000 or more U.S. persons during a 12-month period. *See* 28 C.F.R. § 202.205.

[10] *See* Press Release, U.S. Dep't of Just., *Justice Department Implements Critical National Security Program to Protect Americans' Sensitive Data from Foreign Adversaries* (Apr. 11, 2025) (quoting Deputy Attorney General Todd Blanche), https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-program-protect-americans-sensitive (last accessed, Feb. 11, 2026).

52. *Covered Persons.* The BSDR prohibits transfers when the recipient is a "covered person," defined as any foreign person that is at least 50% owned by, directly or indirectly, a country of concern. *See* 28 C.F.R. § 202.211(a). The People's Republic of China is expressly designated as a country of concern.

53. *Data Brokerage.* Among the transaction types the BSDR regulates is "data brokerage," defined as the sale of data, licensing of access to data, or similar commercial transactions involving the transfer of data from any person to any other person, where the recipient did not collect or process the data directly from the individuals linked or linkable to the data. *See* 28 C.F.R. § 202.214(a).

54. *Prohibitions and Penalties.* The BSDR provides for both civil and criminal penalties for violations, underscoring the national security significance of the rule. See 28 C.F.R. § 202.1301.

G. Google's Cookie Syncing Mechanism Violates the BSDR

55. As described above, Google intercepts users' electronic communications through its advertising infrastructure and transmits persistent identifiers, including the Google GID, IP addresses, and cookie data, to Chinese-affiliated advertising partners through its RTB auction process.

56. These interception, bidding, and syncing practices operate at massive scale. Google's RTB and cookie syncing systems function continuously across thousands of websites, users, and auctions, at a scale that surpasses the 100,000-person threshold that defines bulk transfers under the BSDR.

57. By combining U.S. users' IP addresses and other network-level signals with cookie data and persistent advertising identifiers such as the Google GID, Google transfers covered personal identifiers within the meaning of 28 C.F.R. § 202.212.

58. Google's position in the advertising chain constitutes data brokerage under the BSDR. Google receives user data from publishers' websites and transmits cookie data, advertising identifiers and IP addresses to advertising partners that did not collect or process the data directly from the individuals to whom it relates.

59. The DOJ's own illustrative examples in the Rules confirm that advertising-related data transfers of the kind at issue here constitute prohibited data brokerage. In Example 4, a U.S. company

that operates a mobile app provides IP addresses and advertising IDs of more than 100,000 U.S. users to an advertising exchange based in a country of concern as part of selling advertising space; the DOJ concludes this is a prohibited transaction. 28 C.F.R. § 202.214(b)(4). In Example 5, a U.S. company provides the same data as in Example 4 to a U.S.-based advertising exchange, which then provides it to advertisers headquartered in a country of concern; the DOJ concludes that the U.S. advertising exchange's onward transfer is prohibited data brokerage because the foreign advertisers did not collect or process the data directly from the individuals. 28 C.F.R. § 202.214(b)(5).

60. Google's position in the advertising chain closely parallels the U.S. advertising exchange in Example 5: Google intercepts user data with its embedded software on the U.S. publishers' websites and transmits persistent identifiers and IP addresses to advertising partners headquartered in or subject to the jurisdiction of a country of concern. Google's transfers constitute prohibited data brokerage activity under 28 C.F.R. §§ 202.214 and 202.301(a).

61. Temu qualifies as a "covered person" under 28 C.F.R. § 202.211(a) because it is owned and operated by PDD Holdings Inc., a Chinese company with substantial operations and executive oversight in the People's Republic of China. Although PDD Holdings nominally lists its principal executive offices in Ireland, it maintains a significant presence in China and is subject to Chinese law, including China's National Intelligence Law, Cybersecurity Law, and Data Security Law.[11] These laws compel Chinese companies and individuals to cooperate with government surveillance efforts and grant authorities access to private user data.

62. Pangle qualifies as a "covered person" because it is owned and operated by ByteDance Pte. Ltd., a subsidiary of ByteDance Ltd., a Chinese technology company headquartered in the People's Republic of China. ByteDance is subject to Chinese law and maintains substantial operations

[11] *See also Temu's Dublin Office Raided by EU Regulators on Chinese Subsidy Concerns*, Reuters (Dec. 10, 2025) (last visited Feb. 12, 2026), https://www.reuters.com/sustainability/boards-policy-regulation/temus-irish-facility-raided-by-eu-regulators-concerns-chinese-subsidies-2025-12-10/ ("Temu's European headquarters in Dublin were raided by EU regulators last week on concerns about potential Chinese state subsidies granted to the online retailer, a subsidiary of China's ecommerce giant PDD Holdings . . . .").

in China.[12]

63. MediaGo qualifies as a "covered person" because it is owned and operated by Baidu USA LLC, an affiliate of Baidu, Inc., a China-based technology company headquartered in Beijing that is subject to the People's Republic of China's cybersecurity, data security, and related national security legal frameworks.

64. Because Google's transfers constitute data brokerage under § 202.214, and because they involve bulk sensitive personal data and covered persons, they are prohibited covered data transactions under 28 C.F.R. §§ 202.210 and 202.301(a).

H. Google Had Knowledge of the BSDR and Its Obligations

65. Google has known for over a decade that its real-time bidding system poses serious data security risks. As early as 2014, senior Google executives discussed concerns about whether companies receiving RTB bid requests were reselling the data. The internal discussion concluded that auditing what buyers do with the data is "tough because we mostly send data, not ingest."[13] In January 2021, Google's Chief Marketing Officer wrote to CEO Sundar Pichai urging a strategic shift, explicitly characterizing "real time bidding on user data" as "bad."[14] Pichai did not act on this recommendation. An internal planning document from late 2021 set the objective to "Make RTB

[12] On January 22, 2026, TikTok USDS Joint Venture LLC announced its formation to comply with President Trump's Executive Order signed in September 2025. "The majority American owned Joint Venture will operate under defined safeguards that protect national security through comprehensive data protections, algorithm security, content moderation, and software assurances for U.S. users. … ByteDance retains 19.9% of the Joint Venture." *Announcement from the new TikTok USDS Joint Venture LLC*, TikTok (Jan. 22, 2026) (last visited Feb. 12, 2026), https://newsroom.tiktok.com/announcement-from-the-new-tiktok-usds-joint-venture-llc?lang=en&gad_source=1&gad_campaignid=20482165421&gbraid=0AAAAApbYvmxyx1Oy_mA43lT77GM5tV-AW&gclid=CjwKCAiAkbbMBhB2EiwANbxtbRhnQCP8YHzic1_OX2p0JrUSypYZBRrK6elYM21jMKV9wZ7X7mJWAxoCOPQQAvD_BwE.

[13] Plaintiffs' Exhibit PTX0326, Google Document (Mar. 31, 2016), *United States et al v. Google LLC*, No. 1:23-cv-00108 (E.D. Va. 2023), available at https://www.justice.gov/atr/media/1369416/dl?inline (last accessed, Feb. 12, 2026).

[14] Email from Lorraine Twohill to Sundar Pichai, et al. (Jan. 29, 2021), *United States, et al., v. Google*, No. 1:20-cv-03010 (D.D.C.), available at https://www.justice.gov/d9/2023-11/417790.pdf (last accessed, Feb. 12, 2026).

privacy safe" over the following three years;[15] Google failed to implement it. Instead, in December 2024, Google announced a policy change that was "less prescriptive with partners in how they target and measure ads," loosening prior restrictions on the use of IP addresses and device-level data to identify individual users.[16]

66. Google had actual and constructive knowledge of the BSDR and its prohibitions. Google designed, built, and maintains the advertising infrastructure through which the prohibited data transfers occur, including its cookie syncing systems and real-time bidding platform. Google controls which advertising partners are approved to participate in its ecosystem, what data is transmitted in bid requests, and which partners receive Google identifiers through cookie syncing.

67. Despite this knowledge, Google continued to transmit U.S. user data to Chinese-affiliated entities through its advertising system after the BSDR took effect. This included persistent identifiers, browsing activity, and contextual information about the pages users visited, all collected and shared in real time without users' knowledge.

68. Google's integrations with Pangle, MediaGo, and Temu are deliberate business decisions. Google's conduct is not incidental to its operations but central to its advertising business model.

INJURY TO PLAINTIFF AND CLASS MEMBERS

69. Google's unauthorized interception and foreign transmission of user data has caused actual harm to Plaintiff and Class Members in multiple ways.

70. **Invasion of Privacy.** Plaintiff and Class Members have suffered an invasion of their privacy through the unauthorized interception of their electronic communications and the subsequent transmission of their persistent identifiers to foreign-controlled advertising entities. These communications included browsing activity on websites spanning sensitive categories including

[15] Plaintiffs' Exhibit PTX1069, 2022 AViD Sellside Plan, *United States et al v. Google LLC*, No. 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 (last accessed, Feb. 12, 2026).

[16] Upcoming February update to the platforms program policies, Google Platform Policies Help (Dec. 18, 2024), https://support.google.com/platformspolicy/answer/15610408 (last accessed, Feb. 12, 2026).

health, religion, parenting, finance, and many others. The interception and foreign transmission of these communications violated Plaintiff's and Class Members' reasonable expectation that their browsing activity and associated identifiers would not be intercepted nor transmitted to entities subject to the jurisdiction of foreign adversaries. Google's extensive interception and disclosure of Plaintiff's and Class Members' sensitive communications, online browsing activity, and identifying information would be highly offensive to a reasonable person and constitutes an egregious breach of social norms.

71. **Exposure to Foreign Surveillance and Profiling.** Once transmitted to entities affiliated with Chinese corporate groups, Plaintiff's and Class Members' identifiers and associated browsing data are beyond their control. Under Chinese law, including the National Intelligence Law, the Cybersecurity Law, and the Data Security Law, companies and individuals are required to cooperate with government surveillance efforts and grant authorities access to private user data. Plaintiff's and Class Members' data has been placed in the hands of entities subject to these compelled-disclosure obligations, creating an ongoing risk of foreign government surveillance and profiling.

72. **National Security Harm.** The data transmitted through Google's advertising systems can be used, in the hands of a foreign adversary, to build dossiers on U.S. residents, uncover psychological or financial vulnerabilities, and identify individuals in sensitive roles. This risk is not speculative. Google's bid requests can include content classification codes that categorize the subject matter a user is viewing across sensitive categories including bankruptcy, mental health, substance abuse, sexual conditions, cancer, divorce, and specific religious traditions. Google's RTB infrastructure is also capable of transmitting data broker segments that classify individual users as, among other categories, "decision makers for the Government Industry, specifically National Security and International Affairs," "People who work at companies in aerospace manufacturing," "active military" personnel, and "people who are likely Judges."[17] Other segments identify users by

[17] See 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*, ICCL Enforce at 4, 7 (Nov. 2023), https://www.iccl.ie/wp-content/uploads/2023/11/Americas-hidden-security-crisis.pdf (documenting commercially

estimated income brackets, health conditions and prescription medication use, sexual orientation, ethnicity, political media consumption, and status as a minor.[18]

73. When linked to persistent identifiers and IP addresses, these classifications enable a foreign adversary to associate identified individuals with their most sensitive browsing activity, health conditions, financial circumstances, and professional roles. Investigative reporting has documented that data derived from RTB systems has been purchased on the commercial market and used to track the movements of U.S. military and intelligence personnel to sensitive facilities.[19]

74. **Loss of Control Over Personal Data.** Plaintiff and Class Members have been deprived of the ability to control their sensitive personal information and to protect that information from entities identified by the U.S. government as threats to national security and the safety of U.S. citizens. Personal data, especially persistent identifiers that enable cross-site tracking and profiling, has significant commercial and intelligence value.

75. **Statutory Injury.** Independent of the above harms, Google's violation of the ECPA, including its purposeful violation of the BSDR, has caused Plaintiff and Class Members to suffer statutory injury, entitling them to statutory damages as provided by law.

PLAINTIFF'S EXPERIENCE

76. Plaintiff Jenkins has an Android device, which is persistently linked to her Google account, and she uses the Google Chrome Browser on her Android to conduct her online browsing activities.

77. During the relevant time period, Plaintiff Jenkins visited one or more websites that

---

available Google RTB segments including segment IDs 790212316, 808970298, 735904828, and 6978667300) (last accessed, Feb. 12, 2026), see also Electronic Privacy Information Center & ICCL Enforce, *Complaint and Request for Investigation, In re Google's RTB Practices, filed with the Federal Trade Commission* (Jan. 16, 2025), at 14-16 (cataloguing sensitive Google RTB segment data commercially available for purchase, including segments identifying users by health conditions, income, sexual orientation, ethnicity, political media viewing, minor status, and military branch), available at https://epic.org/wp-content/uploads/2025/01/EPIC-ICCL-Enforce-In-re-Googles-RTB-Complaint.pdf (last accessed, Feb. 12, 2026).

[18] *Id*.

[19] *See* 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/ (last accessed, Feb. 12, 2026).

deployed Google's tracking code.

78. For example, Plaintiff specifically visited www.drugs.com and used the website to communicate and obtain information regarding her personal health history. Plaintiff used the search bar to type text and phrases, and she also used tools and features on the website such as the pill identifier, drug interaction tracker, and symptom checker.

79. Plaintiff did not intend or direct any of these communications to Google.

80. Upon information and belief, during Plaintiff's browsing, Google's tracking code intercepted the substance of her browsing activity, including search terms entered and pages viewed, and transmitted it to Google's DoubleClick infrastructure alongside Plaintiff's identifying cookies, IP address, and device information.

81. Upon information and belief, Google identified Plaintiff and shared Plaintiff's personal information as part of the RTB process and transmitted Plaintiff's Google GID to MediaGo, Pangle, and Temu, and shared with these partners the URLs of the pages Plaintiff viewed (including sensitive medical search terms and the names of the pages she viewed), Plaintiff's IP address, IP-derived geolocation, and cookie data.

82. Plaintiff has no direct relationship with Google's advertising infrastructure and had no meaningful opportunity to detect, review, or prevent Google's acquisition of her browsing activity.

83. Plaintiff did not know, nor had reason to know, that Google surreptitiously collected and disseminated information about her web activity (including her IP addresses) to its partners. Plaintiff did not consent to Google intercepting, reading, or using her communications.

CLASS ACTION ALLEGATIONS

84. Plaintiff brings this action individually and on behalf of all other persons similarly situated pursuant to Rule 23(b)(2) and 23(b)(3) of the Federal Rules of Civil Procedure on behalf of themselves and a Class of others similarly situated, defined as follows:

> **Class**: All individuals in the United States whose electronic communications with websites and apps incorporating Google's advertising technology were intercepted and whose personal information was transmitted by Google to Pangle, MediaGo, Temu, or other covered persons under 28 C.F.R. § 202.211, on or after April 8, 2025.
>
> **Maryland Subclass:** All members of the Class who are residents of

Maryland or whose electronic communications with websites incorporating Google's advertising technology were transmitted from within Maryland.

Excluded from the Class are: (a) Defendant and its officers, directors, employees, subsidiaries, parents, successors, predecessors, and affiliates; (b) the Judge presiding over this action and any member of the Judge's immediate family and staff; (c) any juror assigned to this case; (d) persons who properly execute and file a timely request for exclusion from the Class; (e) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (f) Plaintiff's counsel and Defendant's counsel; and (g) governmental entities.

85. Plaintiff reserves the right to modify, change, or expand the Class definition based upon discovery and further investigation.

86. **Numerosity.** The Class is so numerous that joinder of all members is impracticable. Google's advertising and cookie syncing infrastructure operates across millions of websites and reaches hundreds of millions of users. The Class size is estimated to be in the millions or tens of millions. Class Members can be identified through Google's records.

87. **Commonality and Predominance.** There are questions of law and fact common to the Class that predominate over any questions affecting only individual members. These common questions include:

(a) Whether Google used tracking technologies, including Google Publisher Tag, Google Ad Manager, and DoubleClick infrastructure, to intercept users' electronic communications;

(b) Whether Google used a "device" as defined under 18 U.S.C. § 2510(5) to intercept the contents of communications from Plaintiff and the Class;

(c) Whether Google obtained valid consent from Plaintiff and the Class to intercept and disclose their electronic communications to third parties, including foreign entities;

(d) Whether Google transmitted persistent identifiers, including the Google GID, IP addresses, cookie data, and device identifiers, to Pangle, MediaGo, Temu, or other entities affiliated with the People's Republic of China;

(e) Whether the data transmitted by Google constitutes "bulk U.S. sensitive

personal data" under the BSDR;

(f) Whether Google's transmission of that data to covered persons constitutes a prohibited data brokerage transaction under the BSDR.

(g) Whether Google acted knowingly and intentionally in transmitting the data for the purpose of violating the BSDR and invading users' privacy;

(h) Whether Google's interception and disclosure of users' communications falls within the crime-tort exception to the ECPA's party-consent provision;

(i) Whether any purported consent arguments Google may raise are voided by Md. Code Ann., Cts. & Jud. Proc. § 10-402(c)(3), which carves out an exception when "the communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of this State."

(j) Whether Plaintiff and the Maryland Subclass Members had a reasonable expectation of privacy in their intercepted communications

(k) Whether Plaintiff and Class Members are entitled to damages and other monetary relief, and if so, in what amount; and

88. **Typicality.** Plaintiff's claims are typical of the claims of the other members of the Class. Plaintiff and Class Members had their electronic communications intercepted and their persistent identifiers transmitted to Chinese-affiliated entities without their consent. Plaintiff's claims arise from the same practices and course of conduct that give rise to the claims of the other Class Members and are based on the same legal theories.

89. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously. Plaintiff has no interests that are adverse or antagonistic to those of the Class.

90. **Superiority.** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. The damages suffered by many Class Members may be relatively small compared to the burden and expense of individual litigation, making it difficult for

Class Members to individually redress the wrongs done to them. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications. A class action presents far fewer management difficulties, allows claims to be heard that might otherwise go unheard, and provides the benefits of adjudication, economies of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
Violations of the Electronic Communications Privacy Act
(18 U.S.C. § 2511)
(On Behalf of Plaintiff and the Class)

91. The Electronic Communications Privacy Act prohibits any person from "intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a).

92. The ECPA protects both the sending and receipt of communications and provides a private right of action to any person whose electronic communications are intercepted, disclosed, or intentionally used in violation of 18 U.S.C. § 2511(1)(a). 18 U.S.C. § 2520(a).

93. The transmissions between Plaintiff and Class Members and the websites and mobile apps they visit are "transfers of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and therefore constitute "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

94. The ECPA defines "content" to "include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). The information intercepted here—including full-page URLs, search queries, page titles, and other page-level metadata that reveal the substance of the user's browsing activity—constitutes content under the ECPA.

95. The tracking technologies employed by Google, including Google Publisher Tag, Google Ad Manager, DoubleClick tracking scripts, and cookie syncing pixels, constitute "electronic, mechanical, or other devices" within the meaning of 18 U.S.C. § 2510(5) because they are specifically designed to intercept and acquire the contents of electronic communications.

96. The ECPA defines "interception" as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). Google's tracking technologies are embedded in websites' source code and acquire the contents of users' communications as they are transmitted, in real-time and contemporaneously with the users' browsing activity.

97. Google intentionally distributes and maintains tracking scripts, pixels, and advertising infrastructure on third-party websites that reroute user communications to Google's own servers and to third parties. Google's technologies capture the contents of Plaintiff's and Class Members' interactions with these websites and transmit them to Google and its integrated advertising partners, including foreign buyers.

98. Google's tracker executes automatically within Plaintiff's and Class Members' browsers during the page load process. This code intercepts the contents of users' interactions with websites by rerouting first-party communications, including full URLs, search queries, page titles, and contextual information, to Google and its advertising partners. These interceptions occur as part of the browser's rendering sequence, before users can detect, review, or prevent the transmissions.

99. Plaintiff's and Class Members' communications were intercepted surreptitiously and without their consent. Google did not provide clear or conspicuous notice that user interactions with websites would be surveilled and routed to foreign entities, and Plaintiff and Class Members lack a reasonable means to detect, prevent, or opt out of Google's data collection and sharing with foreign-controlled entities. There was no actual or implied consent under applicable law.

100. Google is not a party to the electronic communications it intercepts. Users direct their communications to the websites they visit, not to Google. Google does not operate these websites, does not provide services to users in connection with these communications, and has no direct relationship with users when deployed on third-party sites. Users do not intend or direct any communication to Google's advertising infrastructure; Google's code, embedded on the website by the publisher, acquires the contents of the user's communication with the website without the user's knowledge. A publisher's decision to embed Google's advertising code on its website may reflect a commercial arrangement between the publisher and Google, but it does not make Google a party to

the separate electronic communications between the website's users and the website's server.

101. Even if Google were deemed to be a party to these communications, which it is not, the "party exception" in 18 U.S.C. § 2511(2)(d) does not apply. Google's interception and use of these communications was undertaken knowingly and intentionally for the purpose of committing a criminal and tortious act, namely, the prohibited transmission of bulk U.S. sensitive personal data to covered foreign persons in violation of the BSDR, 28 C.F.R. Part 202 and invading users' privacy.

102. On and after April 8, 2025, Google knowingly engaged in prohibited data-brokerage transactions with Pangle, MediaGo, and Temu, entities affiliated with ByteDance, Baidu, and PDD Holdings, respectively, in violation of 28 C.F.R. § 202.301(a). Violations of the BSDR are subject to criminal penalties under 28 C.F.R. § 202.1301, as well as civil penalties, underscoring the national security significance of the prohibition.

103. Without the interceptions described herein, Google could not conduct the auctions that produce the BSDR violations. The interception is instrumentally necessary to effectuate the prohibited transfers.

104. Google transmits covered personal identifiers (including the Google GID, IP addresses, cookie data, and device identifiers) in combination with one another to Pangle, MediaGo, and Temu, each of which qualify as a covered person under the BSDR.

105. These transmissions involve the bulk sensitive personal data of more than 100,000 U.S. persons and constitute prohibited data brokerage transactions under 28 C.F.R. §§ 202.210, 202.214, and 202.301(a). Google's violation of the BSDR is independent of the act of interception and supplies the criminal and tortious purpose required to trigger the crime-tort exception under 18 U.S.C. § 2511(2)(d).

106. Because Google knowingly intercepted and disclosed Plaintiff's and Class Members' communications and data to covered foreign persons for the purpose of committing this independent criminal and tortious act, and invading users' privacy, Google is not shielded by the "party" exception under the ECPA.

107. As a direct result of Google's violations, Plaintiff and Class Members are entitled to the sum of the actual damages suffered and the profits obtained by Google as a result of its unlawful

conduct, or statutory damages of $100 per day per violation or $10,000, whichever is greater, as authorized by 18 U.S.C. § 2520(c)(2); (c) punitive damages; and (d) reasonable attorneys' fees and costs.

SECOND CAUSE OF ACTION
Violation of the Maryland Wiretap Act
Md. Code Ann., Cts. & Jud. Proc. §§10-401 *et seq.*
(On Behalf of Plaintiff and the Maryland Subclass)

108. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

109. Maryland's Wiretap Act prohibits: (a) the interception or procurement of another to intercept any wire, electronic or oral communication; (b) the intentional disclosure of the contents of any wire, electronic or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic or oral communication; and (c) the intentional use of the contents of any wire, electronic or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic or oral communication. Md. Cts. & Jud. Proc. Code § 10-402.

110. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose or use, a wire, electronic, or oral communication in violation of the Maryland's Wiretap Act is subject to a civil action for: (a) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (b) punitive damages; and (c) reasonable attorneys' fees and other litigation costs incurred. Md. Cts. & Jud. Proc. Code § 10-410.

111. "Person" includes "any individual, partnership, association, joint stock company, trust, or corporation." Md. Cts. & Jud. Pro. § 10-401(14).

112. Google, is a "person" under the wiretap act.

113. "Intercept" is defined as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 10-401(10).

114. "Contents" is defined as either "any information concerning the identity of the parties to such communication," or any information concerning the "existence, contents, substance, purport,

or meaning of that communication." *Id.* § 10-401(4).

115. "Electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system." *Id.* § 10-401(5)(i).

116. Google intentionally distributes and maintains tracking scripts, pixels, and advertising infrastructure on third-party websites that reroute user communications to Google's own servers and to third parties. Google's technologies capture the contents of Plaintiff's and Class Members' interactions with these websites and transmit them to Google and its integrated advertising partners, including foreign buyers.

117. Google's tracker executes automatically within Plaintiff's and Class Members' browsers during the page load process. This code intercepts the contents of users' interactions with websites by rerouting first-party communications, including full URLs, search queries, page titles, and contextual information, to Google and its advertising partners. These interceptions occur as part of the browser's rendering sequence, before users can detect, review, or prevent the transmissions. The acquisition of such contents constitutes an "intercept[ion]" of "wire," "electronic," or "oral communication[s]" within the meaning of Md. Code Ann., Cts. & Jud. Proc. §§ 10-401(10), 10-402(a).

118. Plaintiff's and Class Members' communications were intercepted surreptitiously and without the consent of all parties, as required by Maryland law. Google did not provide clear or conspicuous notice that user interactions with websites would be surveilled and routed to foreign entities, and Plaintiff and Class Members lack a reasonable means to detect, prevent, or opt out of Google's data collection and sharing with foreign-controlled entities. Because Maryland is an all-party consent jurisdiction, neither Google's purported consent nor the website publisher's consent to the use of Google's tracking code is sufficient to authorize the interception of user communications. The consent of the Plaintiff and Class Members, which was never obtained, was independently required.

119. Google is not a party to the electronic communications it intercepts. Users direct their communications to the websites they visit, not to Google. Google does not operate these websites,

does not provide services to users in connection with these communications, and has no direct relationship with users when deployed on third-party sites. Users do not intend or direct any communication to Google's advertising infrastructure; Google's code, embedded on the website by the publisher, acquires the contents of the user's communication with the website without the user's knowledge. A publisher's decision to embed Google's advertising code on its website may reflect a commercial arrangement between the publisher and Google, but it does not make Google a party to the separate electronic communications between the website's users and the website's server.

120. Even if Google were deemed to be a party to these communications, which it is not, its interception would still violates Maryland's wiretap statute. Maryland law requires the consent of *all* parties to the communication before any party may lawfully intercept. Even as a hypothetical "party" Google has not obtained the consent of the Plaintiff or any Class Member, and it therefore doesn't qualify for the consent exception under Maryland law. Specifically, § 10-402(c)(3) expressly provides that consent is no defense where the communication is intercepted "for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of this State." Google's interception and use of these communications was undertaken knowingly and intentionally for the purpose of committing a criminal and tortious act, i.e., the prohibited transmission of sensitive personal data to foreign entities in bulk, which violates the BSDR and invades users' privacy. Google's conduct falls expressly within the crime-tort exception, defeating any consent-based defense they may assume.

121. On and after April 8, 2025, Google knowingly engaged in prohibited data brokerage transactions with Pangle, MediaGo, and Temu, entities affiliated with ByteDance, Baidu, and PDD Holdings, respectively, in violation of 28 C.F.R. § 202.301(a). Violations of the BSDR are subject to criminal penalties under 28 C.F.R. § 202.1301, as well as civil penalties, underscoring the national security significance of the prohibition.

122. Under Maryland Wiretap Act's crime-tort exception, Google's interception of data enables them to conduct auctions that involve BSDR-prohibited counterparties. Regardless of whether Google is a party to the communication, the transfer of the data to BSDR-prohibited counterparties is a legally distinct offense. In essence, Google has violated the Maryland statute two-

fold. *First,* Google is not a party to the communications and therefore is unable to consent to the interception. *Second,* even if Google were a party to the communications, the transfer of information to BSDR-prohibited counterparties would fall squarely into the crime-tort exception.

123. Google transmits covered personal identifiers (including the Google GID, IP addresses, cookie data, and device identifiers) in combination with one another to Pangle, MediaGo, and Temu, each of which qualify as a covered person under the BSDR.

124. These transmissions involve the bulk sensitive personal data of more than 100,000 U.S. persons and constitute prohibited data brokerage transactions under 28 C.F.R. §§ 202.210, 202.214, and 202.301(a). Google's violation of the BSDR is independent of the act of interception and supplies the criminal and tortious purpose required to trigger the crime-tort exception under Md. Code Ann., Cts. & Jud. Proc. § 10-402(c)(3).

125. Google willfully intercepted Plaintiff's and Class Members' communications without the consent of all parties as required by § 10-402(c)(3), because those interceptions were further undertaken for the purpose of committing criminal and tortious acts, including violations of the BSDR and invasion of users' privacy, Google is liable under the Maryland Wiretap Act and cannot claim any consent-based defense because it never obtained the consent of all parties to the communications; the consent of the website publisher alone is legally insufficient under Maryland's all-party consent framework, and even if all parties had consented, the crime-tort exception in § 10-402(c)(3) would independently strip Google of any consent defense.

126. As a direct result of Google's violations, Plaintiff and Class Members are entitled to actual damages, but not less than liquidated damages computed at the rate of $100 per day for each day of violation, or $1,000, whichever is greater, as authorized by Md. Code Ann., Cts. & Jud. Proc. § 10-410(a)(1) and reasonable attorney's fees and other litigation costs reasonably incurred as authorized by § 10-410(a)(3).

THIRD CAUSE OF ACTION

Common Law Invasion of Privacy – Intrusion Upon Seclusion

(On Behalf of Plaintiff and the Maryland Subclass)

127. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

128. Plaintiff brings this claim on behalf of herself and the Maryland Subclass.

129. Under Maryland law, intrusion upon seclusion is a form of invasion of privacy that occurs where a defendant intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns in a manner that would be highly offensive to a reasonable person.

130. Google intentionally intruded upon Plaintiff's and Maryland Subclass Members' private affairs and concerns by intercepting, collecting, and using their electronic communications and personally identifiable information, including IP addresses, persistent identifiers such as the Google GID and IDE and DSID cookies, browsing history, page views, search terms, geolocation information, and device identifiers. As alleged above, Google's tracking code executes within users' browsers when they visit websites and apps that have implemented Google's advertising technology, intercepts the substance of those users' communications with the websites, and transmits that information to Google's servers and to third-party advertising partners.

131. Google further intruded upon Plaintiff's and Maryland Subclass Members' private affairs by using the intercepted information to conduct real-time bidding auctions, perform cookie-syncing with foreign advertising partners, and transmit persistent identifiers and user data to entities owned by, controlled by, or affiliated with corporate groups subject to the jurisdiction of the People's Republic of China, including Pangle, MediaGo, and Temu.

132. Plaintiff and Maryland Subclass Members had a reasonable expectation of privacy in their online communications and associated identifiers. When they visited health, religious, parenting, financial, and other sensitive websites and apps, they reasonably expected that the URLs they visited, the search terms they entered, the articles they read, their IP-derived locations, and their persistent identifiers would not be secretly intercepted by Google and transmitted to third-party advertising entities—much less to entities subject to the laws of a foreign adversary.

133. This expectation of privacy is reinforced by the federal government's enactment of the Bulk Sensitive Data Rule, through which the Department of Justice determined that the commercial transfer of Americans' persistent identifiers and related sensitive data to entities subject to the jurisdiction of countries of concern, including the People's Republic of China, poses an "unusual and extraordinary threat" to U.S. national security sufficient to warrant categorical prohibition. A reasonable Maryland resident whose own government has determined that such transfers are so dangerous as to be prohibited outright would not expect a technology company to orchestrate them covertly as a byproduct of ordinary web browsing.

134. Google's conduct constitutes a highly offensive intrusion that would be egregious to a reasonable person. Among other things:

(a) The information Google collects and transmits is highly sensitive, including IP addresses revealing approximate location, persistent identifiers enabling cross-site tracking and profiling, and detailed records of users' browsing activity on sites concerning health, religion, parenting, finance, and other intimate aspects of life.

(b) Google's interception and onward transmission occurs invisibly, without clear or conspicuous notice, without any direct relationship with users in connection with these communications, and without any meaningful opportunity for users to review, consent to, or prevent the collection and foreign dissemination of their identifiers and browsing activity.

(c) Google does not merely use this information for domestic commercial advertising purposes; it funnels users' identifiers and related data to entities subject to Chinese laws such as the National Intelligence Law, Cybersecurity Law, and Data Security Law, which may compel cooperation with government surveillance and grant authorities access to private user data, thereby exposing Maryland residents to foreign surveillance and profiling.

(d) Google's conduct monetizes Plaintiff's and Maryland Subclass Members' personal information for Google's own commercial gain, without their knowledge or compensation, by turning private browsing behavior into a commodity sold in high-speed advertising auctions.

135. Plaintiff and Maryland Subclass Members did not consent to Google intercepting their communications with third-party websites, did not consent to Google compiling persistent profiles of

their browsing behavior, and did not consent to Google transmitting their identifiers and associated browsing data to foreign-controlled advertising entities. To the contrary, each of them used websites and apps with the reasonable expectation that their interactions would remain between themselves and the sites they chose to visit.

136. Google's intrusion has caused injury to Plaintiff and Maryland Subclass Members, including but not limited to: (a) the violation of their privacy interests; (b) loss of control over their personal information; (c) exposure of their identifiers and browsing data to entities beyond the protection of U.S. law and subject to the jurisdiction of foreign adversaries; and (d) increased risk of surveillance, profiling, and misuse of their sensitive personal data.

137. Accordingly, Plaintiff and Maryland Subclass Members are entitled to recover damages for the harm to their privacy interests, including compensatory and, where appropriate, punitive damages and such other relief as the Court deems just and proper.

FOURTH CAUSE OF ACTION

Common Law Invasion of Privacy – Publication of Private Facts

(On Behalf of Plaintiff and the Maryland Subclass)

138. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

139. Plaintiff brings this claim on behalf of herself and the Maryland Subclass.

140. Under Maryland law, public disclosure of private facts is a form of invasion of privacy that occurs where a defendant gives publicity to a matter concerning the private life of another that (1) would be highly offensive to a reasonable person and (2) is not of legitimate concern to the public.

141. The electronic communications and data at issue here concern intimate and private matters in the lives of Plaintiff and Maryland Subclass Members. As alleged above, Google's tracking infrastructure intercepts the URLs of pages users view, the search terms they enter, the topics of the articles they read, referrer information, IP addresses, IP-derived geolocation, cookie data, persistent advertising identifiers, and other device and network information. When Maryland residents visit websites such as health information portals, religious resources, parenting and family sites, and

financial sites, these URLs and related signals reveal sensitive details about their health conditions, medications, religious beliefs, family concerns, and financial circumstances.

142. Google gives publicity to these private facts by transmitting users' persistent identifiers and associated browsing activity to multiple third-party advertising entities through its real-time bidding and cookie-syncing systems. Each time a Maryland resident loads a page that uses Google's advertising tools, Google sends bid requests containing the page URL, IP address, location data, cookie data, and audience or content classifications to numerous advertising companies approved to participate in its ecosystem, including entities such as Pangle, MediaGo, and Temu that are owned by, controlled by, or affiliated with corporate groups subject to Chinese jurisdiction.

143. Through this process, Google discloses Plaintiff's and Maryland Subclass Members' private facts—such as that they searched for specific medications or health conditions, read about particular religious topics, or consulted articles on sensitive parenting or financial issues—linked to persistent identifiers and IP-derived locations, to a wide array of advertising partners that have no direct relationship with those individuals. These disclosures are not limited to a single counterparty; they are propagated across Google's advertising network and cookie-syncing relationships in a manner that enables multiple entities to recognize and track the same individuals over time.

144. The facts disclosed are not matters of legitimate public concern. There is no public interest that justifies revealing to foreign-affiliated advertising companies the details of Maryland residents' health-related searches, religious reading habits, parenting concerns, financial worries, or other similarly sensitive browsing activity, tied to persistent identifiers and geolocation data. The disclosures serve only Google's and its partners' commercial interests in targeting and monetizing advertising, not any broader public purpose.

145. Google's disclosures would be highly offensive to a reasonable person. A reasonable Maryland resident would find it deeply objectionable that:

(a) Their browsing of health, religious, parenting, and financial websites is recorded in detail, linked to persistent identifiers and IP-derived locations, and shared with multiple unseen advertising entities with whom they have no relationship.

(b) The entities receiving their data include companies affiliated with corporate groups headquartered in or subject to the jurisdiction of the People's Republic of China, a country designated by the U.S. government as a country of concern, and therefore beyond the protection of U.S. law.

(c) These disclosures occur automatically and invisibly, with no clear or conspicuous notice, no meaningful opportunity to prevent the dissemination, and no practical way to reclaim or delete the data once shared.

146. Plaintiff and Maryland Subclass Members did not consent to Google publicly disclosing their private facts to these advertising partners. They did not authorize Google to share details of their sensitive browsing activity, linked to persistent identifiers and location data, with entities participating in Google's ad auctions or cookie-syncing programs, and they had no reason to anticipate that visiting ordinary consumer websites would result in such disclosures.

147. As a direct and proximate result of Google's public disclosure of their private facts, Plaintiff and Maryland Subclass Members have suffered injury, including the invasion of their privacy, loss of control over sensitive personal information, and exposure of their identities and browsing activity to a broad and largely unknown set of advertising entities, including those subject to foreign surveillance regimes.

148. Accordingly, Plaintiff and Maryland Subclass Members are entitled to recover damages for the harm to their privacy interests, including compensatory and, where appropriate, punitive damages, and such other relief as the Court deems just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the proposed Classes, respectfully requests that this Court:

(a) Certify this case as a class action on behalf of the Classes, appoint Plaintiff as Class representative, and appoint Plaintiff's counsel as Class Counsel;

(b) Declare that Google's actions, as described herein, violate the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq*., Md. Code Ann., Cts.

& Jud. Proc. § 10-410, and constitute a common law invasion of privacy.

(c) Award Plaintiff and the Class statutory damages of $10,000 or $100 per day for each violation of the ECPA, whichever is greater, as provided by 18 U.S.C. § 2520(c)(2)(B);

(d) Award Plaintiff and the Maryland Subclass statutory damages of $100 per day or $1000, whichever is greater, for each violation under Md. Code Ann., Cts. & Jud. Proc. § 10-410;

(e) Award Plaintiff and the Class compensatory damagesdecl;

(f) Award Plaintiff and the Class punitive damages;

(g) Award pre-judgment and post-judgment interest;

(h) Award reasonable attorneys' fees and costs, as allowed by law; and

(i) Grant such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff demands a trial by jury on all claims and issues so triable.

Respectfully submitted,

Dated: February 19, 2026,

By: */s/: William J. Edelman*

William J. Edelman (SBN: 285177)
MILBERG, PLLC
227 West Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (771) 474-1121
Email: wedelman@milberg.com

Heather M. Lopez (SBN: 354022)
MILBERG, PLLC
280 S. Beverly Drive-Penthouse,
Beverly Hills, CA 90212
Telephone: (331) 240-3015
Email: hlopez@milberg.com

Counsel for Plaintiff and the Proposed Class

ClassAction.org
