UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

CHASOM BROWN, et al.,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No. 20-CV-03664-LHK

ORDER DENYING MOTION TO DISMISS

Re: Dkt. No. 82

Plaintiffs Chasom Brown, Maria Nguyen, William Byatt, Jeremy Davis, and Christopher Castillo (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, sue Defendant Google LLC ("Google"). Before the Court is Google's motion to dismiss Plaintiffs' first amended complaint. ECF No. 82. Having considered the parties' submissions and oral arguments, the relevant law, and the record in this case, the Court DENIES Google's motion to dismiss.

I. BACKGROUND

A. Factual Background

Plaintiffs are Google account holders who used their browser in "private browsing mode." ECF No. 68 ("FAC") ¶ 11. Plaintiffs challenge Google's alleged collection of their data while they

were in private browsing mode. *Id.* ¶ 5.

1. Plaintiffs' Use of Private Browsing Mode

Plaintiffs are Google account holders who used their browser in "private browsing mode." *Id.* ¶ 11. In Google's Chrome browser ("Chrome"), private browsing mode is referred to as "Incognito mode." All Plaintiffs used Google's Chrome browser in Incognito mode. *Id.* ¶¶ 168, 173, 178, 183, 188 (stating that Plaintiffs used Chrome in Incognito mode). However, one plaintiff also used a different browser, Apple's Safari browser, in private browsing mode. *Id.* ¶ 173 (stating that Plaintiff Nguyen used Safari in private browsing mode). Furthermore, Plaintiffs seek to represent a class of users of private browsing mode without regard to the specific browser used. *Id.* ¶ 192.

Plaintiffs allege that "users of the Internet enable 'private browsing mode' for the purpose of preventing others . . . from finding out what the users are viewing on the Internet." *Id.* ¶ 162. For example, users often enable private browsing mode in order to visit especially sensitive websites. *Id.* Accordingly, "users' Internet activity, while in 'private browsing mode,' may reveal: a user's dating history, a user's sexual interests and/or orientation, a user's political or religious views, a user's travel plans, a user's private plans for the future (e.g., purchasing of an engagement ring)." *Id.*

2. Google's Alleged Collection of Plaintiffs' Data

Plaintiffs allege that Google collects data from them while they are in private browsing mode "through means that include Google Analytics, Google 'fingerprinting' techniques, concurrent Google applications and processes on a consumer's device, and Google's Ad Manager." *Id.* ¶ 8. According to Plaintiffs, "[m]ore than 70% of all online publishers (websites) use one or more of these Google services."

Specifically, Plaintiffs allege that, whenever a user, including a user in private browsing mode, visits a website that is running Google Analytics or Google Ad Manager, "Google's software scripts on the website surreptitiously direct the user's browser to send a secret, separate

message to Google's servers in California." *Id.* ¶ 63. This message includes six elements, each of which is discussed below.

First, Plaintiffs allege that Google collects duplicate GET requests. Whenever a user visits a webpage, his or her browser sends a message to the webpage's server, called a GET request. *Id.* The GET request "tells the website what information is being requested and then instructs the website to send the information to the user." *Id.* Accordingly, when Google obtains a duplicate GET request, the duplicate GET request "enables Google to learn exactly what content the user's browsing software was asking the website to display." *Id.* The duplicate GET request "also transmits a . . . header containing the URL information of what the user has been viewing and requesting from websites online." *Id.*[1]

Second, Plaintiffs allege that Google collects the IP address of the user's connection to the Internet, which is unique to the user's device. *Id.* When a device is connected to the Internet, the Internet Service Provider (ISP) that is providing the internet connection will assign the device a unique IP address. *Id.* at 18 n.16. Although IP addresses can change over time, the ISP often continues to assign the same IP address to the same device. *Id.*

Third, Plaintiffs allege that Google collects information identifying the browser software that the user is using, including "fingerprint" data. *Id.* Because every unique device and installed application has small differences, images, digital pixels, and fonts display slightly differently for every device and application. *Id.* ¶ 100. Plaintiffs allege that, "[b]y forcing a consumer to display one of its images, pixels, or fonts, online companies such as Google are able to 'fingerprint' their users." *Id.*

Fourth, Plaintiffs allege that Google collects user IDs issued by the website to the user. *Id.*

---

[1] Other courts have similarly described the process by which duplicate GET requests are sent to servers. *See In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 607 (9th Cir. 2020) (describing process by which Facebook's embedded code caused a user's browser to transmit a duplicate GET request to Facebook) [hereinafter "*Facebook Tracking*"]; *In re Google Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125, 130 (3d. Cir. 2015) (describing process by which Google received duplicate GET requests) [hereinafter "*Google Cookie*"].

¶ 63. According to Plaintiffs, "Google offers an upgraded feature called 'Google Analytics User-ID,' which allows Google to map and match the user . . . to a specific unique identifier that Google can track across the web." *Id.* ¶ 69. Plaintiffs allege that "[b]ecause of Google's omnipresence on the web, the use of User-IDs can be so powerful that the IDs 'identify related actions and devices and connect these seemingly independent data points.'" *Id.*

Fifth, Plaintiffs allege that Google collects the geolocation of the user. *Id.* ¶ 63. According to Plaintiffs, Google collects "geolocation data from (1) the Android operating system running on users' phones or tablets and (b) Google applications running on phones (e.g. Chrome and Maps), Google Assistant, Google Home, and other Google applications and services. *Id.* ¶ 105.

Finally, Plaintiffs allege that Google collects information contained in Google cookies, which were saved by the user's browser. *Id.* ¶ 63.[2] According to Plaintiffs, "Google Analytics contains a script that causes the user's . . . browser to transmit, to Google, information from each of the Google Cookies already existing on the browser's cache." *Id.* ¶ 70. These cookies "typically show, at a minimum, the prior websites the user has viewed." *Id.* Thus, Google can obtain a user's browsing history from the current browsing session.

In addition, Plaintiffs allege that, for users using Chrome without Incognito Mode, Chrome constantly transmits "a unique digital string of characters called Google's 'X-Client-Data Header,' such that Google uniquely identifies the device and user thereafter." *Id.* ¶ 95. However, Plaintiffs allege that the X-Client Data Header is not present when a Chrome user has enabled Incognito Mode. *Id.* ¶ 96. Accordingly, Plaintiffs allege that Google is able to tell when a Chrome user has enabled Incognito Mode. *Id.* ¶ 96.

3. Google's Representations to Plaintiffs

Plaintiffs allege that they "reasonably believed that their data would not be collected by

[2] Cookies are "small text files stored on the user's device." *Facebook Tracking*, 956 F.3d at 596. Cookies allow third-party companies like Google "to keep track of and monitor an individual user's web activity over every website on which these companies inject ads." *Google Cookie*, 806 F.3d at 131.

Google and that Google would not intercept their communications when they were in 'private browsing mode'" because of Google's representations regarding private browsing mode. *Id.* ¶ 3. Conversely, Google contends that it disclosed the alleged data collection. ECF No. 82 ("Mot.") at 5–6. Five Google documents are of particular relevance regarding Google's representations to users:[3] (1) Google's Privacy Policy; (2) Chrome's Privacy Notice; (3) a Google webpage entitled "Search & browse privately"; (4) a Google webpage entitled "How private browsing works in Chrome"; and (5) the Incognito Splash Screen. The Court discusses each document in turn.

First, Google's Privacy Policy states: "As you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy." Schapiro Decl. Exh. 1. Google's Privacy Policy states:

> Our Privacy Policy explains:
>
> - What information we collect and why we collect it.
> - How we use that information.
> - The choices we offer, including how to access and update information.

Id.

Google's Privacy Policy in effect from March 25, 2016 to June 28, 2016 made the following disclosures regarding Google's collection of data from users:

> We collect information about the services that you use and how you use them, like when you . . . visit a website that uses our advertising services, or view and interact with our ads and content.
>
> This information includes: . . . device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number).

[3] At the hearing on Google's motion to dismiss, the Court asked the parties to identify the key documents for this motion. Tr. of Feb. 25, 2021 Hearing at 12:23–13:03, ECF No. 104. The parties directed the Court's attention to eight documents, five of which are relevant to the representations Google made to users regarding private browsing and data collection. *Id.* at 15:10–14. Accordingly, the Court focuses on these documents.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.