UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

PATRICK CALHOUN, et al.,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No. 20-CV-05146-LHK

ORDER GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS WITH LEAVE TO AMEND

Re: Dkt. No. 57

Plaintiffs Patrick Calhoun, Elaine Crespo, Hadiyah Jackson, and Claudia Kindler (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' complaint. ECF No. 57. Having considered the parties' submissions and oral arguments, the relevant law, and the record in this case, the Court GRANTS IN PART AND DENIES IN PART Google's motion to dismiss with leave to amend.

I. BACKGROUND

A. Factual Background

1. Google's Alleged Collection of Plaintiffs' Data

Plaintiffs are users of Google's Chrome browser who allege that they "chose not to 'Sync'

their [Chrome] browsers with their Google accounts while browsing the web . . . from July 27, 2016 to the present." ECF No. 1 ("Compl.") ¶ 1. Chrome's Sync feature enables users to store their personal information by logging into Chrome with their Google account. *Id.* ¶ 39.[1]

Plaintiffs allege that "Chrome sends . . . personal information to Google when a user exchanges communications with any website that includes Google surveillance source code . . . regardless of whether a user is logged-in to Google Sync or not." *Id.* ¶ 134 (emphasis omitted). According to Plaintiffs, Google's code "is found on websites accounting for more than half of all internet tracking" and "Chrome is . . . used on a majority [59%] of desktop computers in the United States, giving Google unprecedented power to surveil the lives of more than half of the online country in real time." *Id.* ¶¶ 9, 194.

Plaintiffs allege Google collects five different types of personal information: (1) "The user's unique, persistent cookie identifiers"; (2) "The user's browsing history in the form of the contents of the users' GET requests and information relating to the substance, purport, or meaning of the website's portion of the communication with the user"; (3) "In many cases, the contents of the users' POST communications"; (4) "The user's IP address and User-Agent information about their device"; and (5) The user's X-Client Data Header. *Id.* ¶ 134.

First, according to Plaintiffs, Google collects "[t]he user's unique, persistent cookie identifiers." *Id.* ¶ 134. "A cookie is a small text file that a web-server can place on a person's web browser and computing device when that person's web browser interacts with the website server." *Id.* ¶ 55. According to Plaintiffs, "[c]ookies are designed to and, in fact, do operate as a means of identification for Internet users." *Id.* ¶ 57. Plaintiffs allege that "Google uses several cookies to identify specific Internet users and their devices." *Id.* ¶ 61. Plaintiffs further allege that "Google also engages in a controversial practice known as 'cookie synching' which further allows Google

[1] According to Google, "Chrome offers four modes: (1) Basic Browser; (2) Signed In; (3) Signed In with sync enabled; and (4) Incognito." ECF No. 57 ("Mot.") at 1 n.1. In the instant case, Plaintiffs allege that they used only the first two modes. *Id.* In a related case, *Brown v. Google*, the plaintiffs challenge Google's data collection while they were in private browsing mode, which is called Incognito mode in Chrome. *See* Case No. 20-CV-03664-LHK, ECF No. 168, ¶ 11.

to associate cookies with specific individuals." *Id.* ¶ 62.

Second, Plaintiffs allege that Google collects "[t]he user's browsing history in the form of the contents of the users' GET requests and information relating to the substance, purport, or meaning of the website's portion of the communication with the user." *Id.* ¶ 134. A GET request is one of "[t]he basic commands that Chrome uses to send the users' side of a communication." *Id.* ¶ 114. When a user types a website address or clicks a link to a website, "Chrome contacts the website . . . and sends a [GET request]." *Id.* ¶ 115. According to Plaintiffs, Chrome "[p]laces the contents of [a] GET . . . request in storage in the browser's web-browsing history and short-term memory." *Id.* ¶ 117. Chrome allegedly stores the contents of the communication "so that, if the user's web-browser crashes unexpectedly, when the user re-starts their browser, the browser will be able to offer the user the ability to return to their last communications prior to the browser's crash." *Id.* ¶ 118.

Third, Plaintiffs allege that Google collects "[i]n many cases, the contents of the users' POST communications." *Id.* ¶ 134. Like a GET request, a POST request is one of "[t]he basic commands that Chrome uses to send the users' side of a communication." *Id.* ¶ 114. "If . . . [a] user were filling out a form on [a] website and clicks a button to submit the information in the form, Chrome . . . makes [a] connection with the website server [and] . . . sends a 'POST' request that includes the specific content that the user placed in the form." *Id.* ¶ 116. According to Plaintiffs, Chrome "[p]laces the contents of [a] . . . POST request in storage in the browser's web-browsing history and short-term memory." *Id.* ¶ 117. Chrome allegedly stores the contents of the communication "so that, if the user's web-browser crashes unexpectedly, when the user re-starts their browser, the browser will be able to offer the user the ability to return to their last communications prior to the browser's crash." *Id.* ¶ 118.

Fourth, according to Plaintiffs, Google collects "[t]he user's IP address and User-Agent information about their device." *Id.* ¶ 134. "An IP address is a number that identifies a computer connected to the Internet." *Id.* ¶ 47. "IP addresses of individual Internet users are used by Internet

service providers, websites, and tracking companies to facilitate and track Internet communications." *Id.* ¶ 50. Plaintiffs allege that "Google tracks IP addresses associated with specific Internet users" and "associate[s] specific users with IP addresses." *Id.* ¶¶ 51–52. Plaintiffs further allege that "[b]ecause Google collects the IP Address and user agent information together, Google can identify a user's individual device even if more than one device shares the same IP address." *Id.* ¶ 54.

Finally, Plaintiffs allege that Google collects the user's X-Client Data Header. *Id.* ¶ 134. The X-Client Data Header "is an identifier that when combined with IP address and user-agent, uniquely identifies every individual download version of the Chrome browser." *Id.* ¶ 69. Plaintiffs allege that, as of March 6, 2018, the X-Client Data Header "is sent from Chrome to Google every time users exchange an Internet communication, including when users log-in to their specific Google accounts, use Google services such as Google search or Google maps, and when Chrome users are neither signed-in to their Google accounts nor using any Google service." *Id.* ¶ 70.

2. Google's Representations to Plaintiffs

According to Plaintiffs, "Google expressly promises Chrome users that they 'don't need to provide any personal information to use Chrome,' and that '[t]he personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google Account by turning on sync[.]'" *Id.* ¶ 2. Conversely, Google contends that it explicitly disclosed the alleged data collection. Mot. at 3–5. Four documents are of particular relevance regarding Google's representations to users: (1) Google's Terms of Service; (2) Google's Privacy Policy; (3) Chrome's Terms of Service; and (4) Chrome's Privacy Notice. The Court discusses each document in turn.

First, as of March 31, 2020, Google's Terms of Service stated that the "Terms of Service help define Google's relationship with you as you interact with our services." Compl. Exh. 4. Google's Terms of Service state that "[u]understanding these terms is important because, by using our services, you're agreeing to these terms." *Id.* Prior versions of Google's Terms of Service

made similar statements.

From April 14, 2014 until March 31, 2020, Google's Terms of Service invoked Google's Privacy Policy as follows: "You can find more information about how Google uses and stores content in the privacy policy or additional terms for particular services." Compl. Exh. 2, 3. As of March 31, 2020, Google's Terms of Service explicitly excluded Google's Privacy Policy: "Besides these terms, we also publish a Privacy Policy. Although it's not part of these terms, we encourage you to read it to better understand how you can update, manage, export, and delete your information" Compl. Exh. 4.

Google's Terms of Service also invoke Google's service-specific terms and policies: "Next to each service, we also list additional terms and policies that apply to that particular service. The Terms of Service, additional terms, and policies define our relationship and mutual expectations as you use these services." *Id*.

Finally, Google's Terms of Service state that "California law will govern all disputes arising out of or relating to these terms, service-specific additional terms, or any related services, regardless of conflict of laws rules." Compl. Exh. 4.

Second, Google's Privacy Policy states: "[A]s 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." Compl. Exh. 7. 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 June 28, 2016 to August 29, 2016 made the following disclosures regarding Google's collection of data from users:

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.