

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

PATRICK CALHOUN, ET AL.

Plaintiffs,

v.

GOOGLE, LLC,

Defendant.

CASE NO. 20-cv-5146-YGR
**ORDER GRANTING GOOGLE’S MOTION
FOR SUMMARY JUDGMENT; DENYING
PLAINTIFFS’ MOTION FOR CLASS
CERTIFICATION AS MOOT; AND ORDER RE
PENDING ADMINISTRATIVE MOTIONS**
Re: Dkt. Nos. 340, 395, 425, 427, 488, 855,
909

Plaintiffs Patrick Calhoun, Elaine Crespo, Michael Henry, Cornice Wilson, Rodney Johnson, and Claudia Kindler bring this suit against defendant Google, LLC based on Google’s alleged data collection practices and use of data from “users who chose not to ‘Sync’ their Google accounts with Chrome while browsing the web.” (Dkt. 162-3, First Amended Complaint, “FAC”, ¶ 1.)¹ Six alleged claims remain: (1) violation of the California Invasion of Privacy Act (Count Five); (2) intrusion upon seclusion (Count Seven); (3) breach of contract (Count Eight); (4) breach of the implied covenant of good faith and fair dealing (Count Nine); (5) statutory larceny (Count Thirteen); and (6) violation of California’s Unfair Competition Law (Count Fourteen).

Pending before the Court is Google’s Motion for Summary Judgment on Consent (Dkt. No. 395, “Mot.”) and plaintiffs’ Motion for Class Certification (Dkt. 340, “Class Cert. Mot.”). Having carefully considered the parties’ briefing, the admissible evidence, the record in this case, and upon further consideration after oral argument which occurred on August 26, 2022, and the evidentiary hearing which occurred on October 24, 2022, Google’s Motion for Summary Judgment is hereby **GRANTED** and plaintiffs’ Motion for Class Certification is **DENIED AS MOOT**.²

¹ There are also two related actions pending in front of this Court: *Brown et al. v. Google LLC*, 20-3664, which deals with Google’s alleged surreptitious interception and collection of personal and sensitive user data while users are in “private browsing mode,” and *In re Google RTB Consumer Privacy Litigation*, 21-2155, which focuses not on collection but on Google’s alleged sharing and selling of consumers’ personal information through its Real-Time Bidding (“RTB”) system.

² Also pending before the Court is plaintiffs’ Motion for Leave to Supplement the Briefing

I. BACKGROUND**A. Alleged Data Collection and Use**

Plaintiffs' FAC alleges as follows:

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." (FAC ¶ 1.) Chrome's Sync feature allows users to store their personal information by logging into Chrome with their Google account. (*Id.* ¶ 45.) Google promises users that they need not provide any personal information to use Chrome and that any information that Chrome stores will not be sent to Google unless one syncs their account. (*Id.* ¶ 3.) However, Google "intentionally and unlawfully causes Chrome to record and send users' personal information to Google regardless of whether a user elects to Sync or even has a Google account." (*Id.*)

The personal information collected and sent to Google includes: (i) "unique, persistent cookie identifiers"; (ii) "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"; (iii) "the contents of the users' POST communications"; (iv) "the user IP address and User-Agent information about their device"; and (v) "the user's x-client-data identifier", (collectively, "at-issue" data). (*Id.* ¶ 141.)

Plaintiffs also allege that Google improperly uses the at-issue data. According to plaintiffs, Google engages in "cookie-syncing" whereby "first-party cookies are set by websites with which users are directly interacting, but then those first-party websites also pass that cookie value [] along to Google Analytics, where Google takes the personal information it has about the user's

Regarding Remedies, Dkt. No. 855, plaintiffs' Administrative Motion for Leave to Supplement the Record as to Google's Motion for Summary Judgment and to File a Sur-Reply, Dkt. No. 909, and several administrative motions to seal. Having denied plaintiffs' Motion for Class Certification as moot, the Motion to Supplement the Briefing Regarding Remedies is also **DENIED AS MOOT**. Plaintiffs' Motion for Leave to Supplement the Record and File a Sur-Reply as to Summary Judgment is also **DENIED**. The evidence plaintiffs seek to proffer is similar to evidence that already exists in this case. Therefore, the Court finds supplementation of the record or additional briefing unnecessary.

As to the administrative motions to seal, these motions are **DENIED** to the extent the information is referenced and included in this Order. The specific motions will be addressed by separate court order.

particular browser and links the Google Analytics first-party cookie information to Google’s own third-party cookies and the user’s browsing.” (*Id.* ¶ 69.) Google also allegedly “combine[s] . . . personal information that it obtained when [users are] not logged-in to Google sync with other data it has about [users]” “to create detailed dossiers about individual’s personal information” for targeted advertising. (*Id.* ¶¶ 174, 180, 186, 258.)

The FAC defines a proposed class as all persons residing in the United States whose personal information was collected by Google when they used Google’s Chrome browser and chose not to Sync their browser with any Google account, with a class period of July 27, 2016 to the present. (*Id.* ¶ 262.)

B. Google’s Representations and Disclosures

Relevant for this motion, the parties represent that the following different policies govern the conduct alleged herein: (1) Google’s General Terms of Use (“General ToS”) and Google’s related Privacy Policy (“General Privacy Policy”); (2) Chrome Privacy Notice; (3) Consent Bump Agreement; and (4) New Account Creation Agreement. These agreements contain several representations and disclosures. Relevant portions are discussed herein.

1. General ToS and General Privacy Policy

Google’s General ToS provides that it describes “what [one] can expect from [Google] as [they] use Google services” and “helps define Google’s relationship with [users].” (Dkt. No. 462, Barnes Declaration “Barnes Decl.,” Ex. 32 at 1.) Further, “understanding these terms is important because, by using our services, you’re agreeing to these terms.” *Id.* Plaintiffs also invoke Google’s specific terms and policies for specific Google services. (*Id.* at 2.) Relevant here, a hyperlink is included to a list of services and their additional service-specific terms, including the Chrome Privacy Notice. (*Id.*) The General ToS states that where “these terms conflict with the service-specific additional terms, the additional terms will govern for that service.” (*Id.* at 14.)

Prior to March 31, 2020, Google’s General ToS incorporated Google’s General Privacy Policy. (*See e.g.*, Dkt. No. 2, Exhibits of Original Complaint, “Compl. Exs.,” at Exs. 2-5.)

Google’s General 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.” (*Id.* at Ex. 7.)

The General Privacy Policy in effect at the beginning of the class period made the following disclosures regarding Google's collection of data from users:

Information we get from your use of our services. 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 information . . . such as your hardware model, operating system version, **unique device identifiers**, and mobile network information . . . **Google may associate your device identifiers . . . with your Google Account.**
- Log information. . . [w]hen you use our services or view content provided by Google, we automatically collect and store certain information in server logs. This includes:
 - **details of how you used our service, such as your search queries . . .**
 - **Internet protocol address.**
 - **device event information such as . . . the date and time of your request and referral URL.**
 - **Cookies that may uniquely identify your browser or your Google Account.**

Cookies and similar technologies.

We and our partners use various technologies to collect and store information when you visit a Google service, and this may include using cookies or similar technologies to identify your browser or device. We also use these technologies to collect and store information when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites. When used in conjunction with our advertising services, such as those using the DoubleClick cookie, Google Analytics **information is linked**, by the Google Analytics customer or by Google, using Google technology, **with information about visits to multiple sites.**

Information we collect when you are signed in to Google, in addition to information we obtain about you from partners, **may be associated with your Google Account.** When information is associated with your Google Account, we treat it as personal information.

How we use information we collect.

We use the information we collect from all of our services . . . to offer you tailored content –like giving you more relevant search results and ads.

We use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services. One of the products we use to do this on our own services is Google Analytics. For example, by saving your language preferences, we'll be able to have our services appear in the language you prefer. When showing you tailored ads, we will not associate an identifier from cookies or similar technologies with sensitive categories, such as those based on race, religion, sexual orientation or health.

We may combine personal information from one service with information, including personal information, from other Google services – for example to make it easier to share things with people you know. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

“linked with information about visits to multiple sites”

Google Analytics is based on first-party cookies. Data generated through Google Analytics can be linked, by the Google Analytics customer or by Google, using Google technology, to third-party cookies, related to visits to other websites, for instance when an advertiser wants to use its Google Analytics data to create more relevant ads, or to further analyze its traffic.

[Learn more.](#)

“your activity on other sites and apps”

This activity might come from your use of Google products like Chrome Sync or from your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics). **These products share information about your activity with Google and, depending on your account settings and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information.**

Learn more.

(*Id.*) (Emphasis supplied.) Subsequent versions of Google’s General Privacy Policy made similar disclosures. (*Id.* at Exs. 8-16; Dkt. No. 393-3, Fair Declaration, “Fair Decl.,” at ¶¶ 56-58.) In addition to explaining that Google collects “activity on third-party sites and apps that use our services,” Google also disclosed in subsequent policies that one’s “Chrome browsing history you’ve synced with your Google Account” is also collected. (Compl. Exs., at Ex. 16.) The General Privacy Policy “applies to all of the services offered by Google Inc. and its affiliates” and services offered on other sites (such as Google’s advertising services) but excludes those services that have a separate privacy policy that does not incorporate the General Privacy Policy. (*Id.* at Ex. 7 at 5.)

2. *Chrome Privacy Notice*

The Chrome Privacy Notice, which is incorporated into both the General ToS and the General Privacy Policy, invites users to “learn how to control the information that’s collected, stored, and shared when you use the Google Chrome browser.” (Barnes Decl., Ex. 33 at 1.) The policy states that it “describes features that are specific to Chrome” and that “any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the Google Privacy Policy.” (*Id.*) Relevant here, the Chrome Privacy Notice contains the following disclosures:

You don’t need to provide any personal information to use Chrome, but Chrome has different modes you can use to change or improve your browsing experience. Privacy practices are different depending on the mode you’re using.

The basic browser mode stores information locally on your system. This information might include: . . . browsing history information. For example, Chrome stores the URLs of pages that you visit, a cache of texts, images and other resources from those pages . . . cookies or data from websites you visit . . . [and] a record of what you downloaded from websites.

The 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 . . .

Information for website operators. Sites that you visit using Chrome will automatically receive standard log information, including your system’s IP address and data from cookies. In general, the fact that you use Chrome to access Google

services, such as Gmail, does not cause Google to receive any additional personally identifying information about you.

Identifiers in Chrome. Chrome includes a number of unique and non-unique identifiers necessary to power features and functional services. For example, if you use push messaging, an identifier is created in order to deliver notices to you. Where possible, we use non-unique identifiers and remove identifiers when they are no longer needed. Additionally, the following identifiers help us develop, distribute, and promote Chrome, but are not directly related to a Chrome feature.

- [. . .]
- [. . .]
- **Field trials. We sometimes conduct limited tests of new features. Chrome includes a seed number that is randomly selected on first run to assign browsers to experiment groups. Experiments may also be limited by country (determined by your IP address), operating system, Chrome version, and other parameters. A list of field trials that are currently active on your installation of Chrome is included in all requests sent to Google. Learn more.**

When you sign in to the Chrome browser or a Chromebook and enable sync with your Google Account, your personal information is saved in your Google Account on Google's servers so you may access it when you sign in and sync to Chrome on other computers and devices. This personal information will be used and protected in accordance with the [Google Privacy Policy](#). This type of information can include:

- Browsing history,
- Bookmarks,
- Tabs,
- Password and autofill information,
- Other browser settings, like installed extensions

Sync is only enabled if you choose.

Server Log Privacy Information.

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your **web request, Internet Protocol address**, browser type, browser language, the date and time of your request and **one or more cookies that may uniquely identify your browser.**

More information

Information that Google receives when you use Chrome is used and protected under the [Google Privacy Policy](#). Information that other website operators and add-

on developers receive, including cookies, is subject to the privacy policies of those websites.

Key terms

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about how Google uses cookies and how Google uses data, including cookies, when you use our partners' sites or apps.

(*Id.*) (Emphasis supplied.) As indicated above, the Chrome Privacy Notice includes a link to the General Privacy Policy.

3. *Consent Bump Agreement*

The Consent Bump Agreement is a push down banner that Google showed to account holders either when they visited a “Google owned-and-operated property” while signed into their account or when users signed into their account for the first time after June 2016. (Dkt. No. 393-4, Gregory Fair Decl., ¶¶ 16-19.) Google launched the Consent Bump Agreement in June 2016.

(*Id.*) A depiction when it was first launched is included as Appendix A. The Consent Bump Agreement explained that Google had introduced “some new features for your Google Account” and that:

when you used Google services like Search and YouTube, you generate data—things like what you’ve searched for and videos you’ve watched. You can find and control that data in My Account under the Web & App Activity setting. With this change, this setting may also include **browsing data from Chrome and activity from sites and apps that partner with Google, including those that show ads from Google.**

(*Id.*) (Emphasis supplied.) Further, it explained that “Google will use this information to make ads across the web more relevant for you.” (*Id.*)

The Consent Bump Agreement included a link to a Frequently Asked Questions (“FAQs”) page through the “Learn More” link. (Fair Decl., at ¶ 23.) The FAQ page stated in relevant part:

Many websites and apps use Google technologies to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like partners who use **Google Analytics to improve the ads they show**).

As you use these sites, **your web browser may send certain information to Google that may include the web address of the page that you're visiting, your IP address, or cookies previously set by the site or Google.**

(*Id.* at Ex. 3 at GOOG-CABR-04067841) (Emphasis supplied.)

Customers were then provided choices. The options allowed a user to: “Choose I AGREE to turn these features on or MORE OPTIONS for more choices.” (*See id.* at Ex. 3, at GOOG-CABR-04067836.) If the user selected “I AGREE,” the new settings were turned on. (Fair Decl., ¶ 24.) Alternatively, if the user selected “MORE OPTIONS,” the user was taken to a screen that offered several options, including “No changes- continue on your way”; “No changes -review key privacy settings more fully”; or “Yes, I’m in- turn on these new features.” (*Id.*)

4. *New Account Creation Agreement*

Finally, beginning around June 2016, Google also updated its New Account Creation Agreement, which required users creating new accounts to agree to certain disclosures. (*Id.* at ¶ 32.) A depiction of this agreement when it was first launched is included as Appendix B.

The New Account Creation Agreement incorporates Google’s General Terms of Service and General Privacy Policy and states, “[b]y choosing ‘I agree’ below you agree to Google’s Terms of Service. You also agree to our Privacy Policy, which describes how we process your information” (*Id.*)

The New Account Creation Agreement discloses the “data we process when you use Google.” Specifically, the agreement explained:

- When you use Google services to do things like write a message in Gmail or comment on a YouTube video, we store the information you create.
- When you search for a restaurant on Google Maps or watch a video on YouTube, for example, **we process information about that activity—including information like the video you watched, device IDs, IP addresses, cookie data, and location.**
- **We also process the kinds of information described above when you use apps or sties that use Google services like ads, Analytics, and the YouTube video player.**

- Depending on your account settings, some of this data may be associated with your Google Account and we treat this data as personal Information. You can control how we collect and use this data at My Account (myaccount.google.com).

Additionally, it explains why the collected information is processed, including to:

- Help our services deliver more useful, customized content such as more relevant search results;
- Improve the quality of our services and develop new ones;
- **Deliver personalized ads, both on Google services and on sites and apps that partner with Google;**
- Improve security by protecting against fraud and abuse; and
- **Conduct analytics and measurement to understand how our services are used.**

The New Account Agreement also explains that data is combined across services:

We also combine data among our services and across your devices for these purposes. For example, we show you ads based on information from your use of Search and Gmail, and we use data from trillions of search inquiries to build spell-correction models that we use across all of our services.

(*Id.*) (Emphasis supplied.) The New Account Agreement requires users to either click “I Agree or Cancel.” (*Id.*)

In May 2018, Google modified the New Account Creation Agreement to include more disclosures about how information is combined. (*See id.* ¶ 37.) The modified New Account Agreement explains that “[Google] show[s] you ads based on information about your interests, which we can derive from your use of Search and YouTube.” (*Id.* at Ex. 22.) The modifications also include the addition of a paragraph titled “You’re in Control” and a “MORE OPTIONS” link to make it easier for users to adjust their settings. (*Id.* at Exs. 22-23.) The “You’re in Control” language states:

Depending on your account settings, some of this data may be associated with your Google Account and we treat this data as personal information. You can control how we collect and use this data now by clicking “More Options” below. You can always adjust your controls later or withdraw your consent for the future by visiting My Account (myaccount.google.com).

(*Id.* at Ex. 22.)

II. LEGAL STANDARD

A party may move for summary judgment on a “claim or defense.” Fed. R. Civ. P. 56(a). Summary judgment is appropriate when “there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(a). As a general matter, where the party moving for summary judgment would bear the burden of proof at trial, that moving party bears the initial burden of proof at summary judgment as to each material fact to be established in the complaint and must show that no reasonable jury could find other than for the moving party. *See S. California Gas Co. v. City of Santa Ana*, 336 F.3d 885, 888 (9th Cir. 2003) (*citing* William W Schwarzer, et al., CALIFORNIA PRACTICE GUIDE: FEDERAL CIVIL PROCEDURE BEFORE TRIAL (Rutter Group) § 14:124–127 (2001)).

If the moving party satisfies its initial burden, the burden then shifts to the opposing party to establish the existence of material disputes of fact that may affect the outcome of the case under the governing substantive law. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). The non-moving party must “identify with reasonable particularity the evidence that precludes summary judgment.” *Keenan v. Allan*, 91 F.3d 1275, 1279 (9th Cir. 1996). Indeed, it is not the duty of the district court “to scour the record in search of a genuine issue of triable fact.” *Id.* “A mere scintilla of evidence will not be sufficient to defeat a properly supported motion for summary judgment; rather, the nonmoving party must introduce some significant probative evidence tending to support the complaint.” *Summers v. Teichert & Son, Inc.*, 127 F.3d 1150, 1152 (9th Cir. 1997) (citation and internal quotation marks omitted). If the non-moving party fails to make this showing, the moving party is entitled to summary judgment. *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986).

When deciding a summary judgment motion, a court must view the evidence in the light most favorable to the nonmoving party and draw all justifiable inferences in its favor. *Anderson*, 477 U.S. at 255.

///

///

///

III. GOOGLE’S MOTION FOR SUMMARY JUDGMENT ON CONSENT

A. “Consent” Framework

Google contends that plaintiffs’ remaining claims are barred because plaintiffs consented to Google’s receipt and use of the at-issue data. More specifically, consent is a defense to:

(1) violation of the California Invasion of Privacy Act (“CIPA”) (Count Five) by the plain terms of the statute, Cal. Pen. Code §§ 631(a), 632(a) (prohibiting wiretapping and eavesdropping “without the consent of all parties to the communication”);

(2) intrusion upon seclusion (Count Seven), *see Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 955–56 (N.D. Cal. 2017), *aff’d*, 745 F. App’x 8 (9th Cir. 2018) (“Plaintiffs’ consent . . . bars their common-law tort claims [for intrusion upon seclusion]”);

(3) breach of contract (Count Eight); and (4) breach of the implied covenant of good faith and fair dealing (Count Nine); *see In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 792, 801–803 (N.D. Cal. 2019) (dismissing plaintiffs’ breach of contract claim and parallel breach of the implied covenant of good faith and fair dealing claims, explaining that plaintiffs consented to the conduct of “allowing standard app developers to obtain user information through users’ friends” when they created their Facebook accounts);

(5) statutory larceny (Count Thirteen) by the plain terms of the statute, *see People v. Brock*, 143 Cal. App. 4th 1266, 1274 (2006) (“Theft by larceny . . . is not committed when the property is taken with the owner’s consent.”); and

(6) violation of California’s Unfair Competition Law (“UCL”) (Count Fourteen), which is predicated on Google’s representations and plaintiffs’ other claims.

Consent may be an element of a claim but it is also “an affirmative defense for which defendant bears the burden of proof.” *Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1044 (9th Cir. 2017).

Consent “can be [express] or implied, but any consent must be actual.” *In re Google, Inc.*, 2013 WL 5423918, at *12 (N.D. Cal. Sept. 26, 2013). Consent is only effective if the person alleging harm consented “to the particular conduct, or to substantially the same conduct” and if the alleged tortfeasor did not exceed the scope of that consent. Restatement (Second) of Torts § 892A

(1979) §§ 2(b), 4 (“no one suffers a legal wrong as the result of an act to which . . . he freely consents”). For consent to be actual, the disclosures must “explicitly notify” users of the conduct at issue. *In re Google, Inc.* at *13; *see also Campbell v. Facebook, Inc.*, 77 F. Supp. 3d 836, 847–48 (N.D. Cal. 2014) (explaining that, for a finding of consent, the disclosures must have given users notice of the “specific practice” at issue).

B. Undisputed Facts Regarding Types of Data Collected

The parties do not dispute that plaintiffs agreed to the agreements discussed above when plaintiffs either created new Google accounts or when they signed into their existing accounts after June 2016. (*See* Fair Decl., ¶¶ 18-55; *id.* at Ex. 3 at 6.)³ The core issues are: which agreement controls the at-issue data collection, and to the extent consent exists, whether it is effective. Plaintiffs contend that the Chrome Privacy Notice applies because they are Chrome users using the Chrome browser. Google disagrees. It argues that because the data collection at issue (except for the X-client-data header) is “browser-agnostic,” Google’s general policies apply. The Chrome Privacy Notice only applies to “features specific to Chrome” and the features at issue are not specific to Chrome.

To better understand the parties’ positions, and to have a more fulsome record on the

³ While plaintiffs argue that the Fair Declaration is facially inadmissible because it is not based on personal knowledge, they do not mount an actual attack on the substance of the declaration, nor do they dispute that they agreed to the various agreements discussed in the declaration.

In any event, plaintiffs’ motion to strike the Fair Declaration does not persuade. Gregory Fair explains in his declaration that he worked as a Product Manager with Google’s Privacy and Data Protection Office and that the regular course of his duties included “manag[ing] . . . Google’s framework for obtaining user consent . . . review[ing] and approv[ing] related disclosures, including disclosure to users about Google’s data collection practices.” (Fair Decl., ¶ 1.) Mr. Fair also explains that he is “familiar with the consent process that Google launched in or around June 2016 to obtain the consent of Google Account holders, like plaintiffs, to store the data at issue in their Google Accounts and use it to personalize ads.” (*Id.*) Thus, Mr. Fair has demonstrated that he has personal knowledge and can testify about the information contained in his declaration.

Plaintiffs’ objection that Mr. Fair was merely “informed” about certain issues does not warrant striking the declaration. (*See* Fair Decl., ¶¶ 2, 3, 28-31, 46-49, 71.) Plaintiffs do not dispute this information, so the fact that Mr. Fair was informed of it does not render his declaration inadmissible. Plaintiffs remaining arguments about the inadmissibility also do not persuade. Much of those arguments elevate form over substance. Accordingly, plaintiffs’ request to strike the Fair Declaration is **DENIED**.

fundamental issue of whether the data collection at-issue is specific to Chrome or browser-agnostic, the Court held an evidentiary hearing. The hearing lasted approximately 7.5 hours and included live testimony from eight witnesses.

For the reasons set forth below, the Court finds no dispute exists that the collection of the at-issue data, except for the X-client-data identifier, is browser-agnostic. The evidence shows that plaintiffs now complain not about the type or nature of the data but the quantity and its use.

Google's expert, Dr. Georgios Zervas, an associate professor of marketing at Boston University's Questrom School of Business, testified that all categories of the at-issue data are collected irrespective of the browser one uses.⁴ (Dkt. No. 911, Evidentiary Hearing Transcript-Part 1, "Evidentiary Tr. Part One", at 51:9-14.) To support his opinion, Dr. Zervas started with a tutorial on how the Internet works.

In the tutorial, Dr. Zervas explained how browsers work and how they request websites. (Evidentiary Tr. Part One, at 36:7-49:23.) Plaintiffs' expert, Dr. Zubair Shafiq, Associate Professor of Computer Science at University of California, Davis, did not dispute these basic concepts. (*Id.* at 81:6-82:6.) When a user types a website URL into an address bar, the browser sends a "HTTP Request"⁵ to the website server in order to retrieve information. (*Id.* at 37:19-40:1.) Precisely because of this standardization, different browsers can communicate with websites in the same way to load the same webpages. (*Id.* at 37:19-38:1.)

Next, Dr. Zervas testified that he analyzed named-plaintiffs' data which consisted of approximately 80GB of server log files. (*Id.* at 50:10-51:5.) The server logs contained record data about plaintiffs' visits to websites using Google's third party services. (*Id.*) He conducted testing on that data which confirmed that the at-issue data is transmitted to Google regardless of the browser used. (*Id.* at 51:9-14.) Because plaintiffs used different browsers, Dr. Zervas was able to

⁴ In this order, where the Court refers to the "at-issue data being browser-agnostic" that includes all of the data *except* for the X-client-data identifier (also referred to as the X-client-data header). The parties agree that the X-client-data identifier is specific to Chrome.

⁵ HTTP is short for Hypertext Transfer Protocol. *See* <https://www.techopedia.com/definition/2336/hypertext-transfer-protocol-http> (last visited December 9, 2022).

1 compare the transmission from Chrome browsers and non-Chrome browsers (Safari, Edge, and
2 Firefox). (*Id.* at 51:1-5.) In comparing the transmissions, he testified that one’s user-agent, URL,
3 IP address, and cookie identifiers were all sent to Google when users visited sites that used
4 Google’s services irrespective of the browser being used. (*Id.* at 51:9-15.)

5 Next, Dr. Zervas conducted another type of testing where he adjusted settings in different
6 browsers to make them more like Chrome and also adjusted the settings in Chrome to have
7 Chrome perform more like other browsers. (*Id.* at 55:5-56:7.) In doing so, he reached the same
8 conclusion. The at-issue data transmissions are the same irrespective of the browser. (*Id.* at 57:10-
9 19.)

10 Similarly, plaintiffs’ expert, Dr. Shafiq, ultimately testified that, with the exception of the
11 X-client-data header, the at-issue data is collected and transmitted to Google by all the major
12 browsers. (Dkt. No. 912, Evidentiary Hearing Transcript- Part 2, “Evidentiary Tr. Part Two”, at
13 308:14-318:15.) Dr. Shafiq does not dispute that the at-issue data is collected irrespective of the
14 browser used.

15 This is confirmed by Dr. Shafiq’s own analysis. By comparing the same kinds of data
16 across browsers one necessarily concedes that the data is in fact collected. Thus, the Court finds
17 plaintiffs’ focus has shifted. Dr. Shafiq agreed that Google receives IP addresses, URLs, and user
18 agents *irrespective of the browser* but now emphasizes that the data is “qualitatively” and
19 “quantitatively” different. (*Id.*) For instance, Dr. Shafiq testified that the amount of information
20 contained in these sources as sent from Chrome is greater than the amount of information sent in
21 other browsers. (*Id.*) Next, he admitted that all browsers send first party cookies. (*Id.* at 310:12-
22 311:10.) The new focus is that Chrome’s first party cookies tend to last longer than other
23 browsers’ cookies. (*Id.* at 311:11-13.)⁶ Dr. Shafiq also testified that all browsers send GET and
24 POST communications but that the information in other browsers are not as detailed and specific
25

26 ⁶ He also testified that some browsers like Firefox and Edge block third party cookies in
27 their default settings and Chrome does not. That said, plaintiffs’ expert, Richard Smith, owner of
28 Boston Software Forensics LLC, testified that while Safari, Edge, and Firefox block third party
cookies in many cases, there are still instances where these browsers send them to Google. (*Id.* at
255:11-256:5.) Google’s expert, Michael Kleber, principal software engineer for Chrome, also
testified to the same. (*Id.* at 222:1-223:2.)

1 as the information in the Chrome browser because other browsers do not send the full URLs. (*Id.*
2 at 317:4-7.)

3 To reinforce the proposition that the same kind of data is collected by all browsers, Glenn
4 Bernston, Engineering Director and Lead of the Google Ad Manager team, testified that Google
5 designs its javascript and software developer kits to comport with industry standards, such as
6 HTTP, so that publishers can build their webpages to work the same regardless of the browser one
7 uses. (Evidentiary Tr. Part One, at 139:1-141:1.) Thus, Google also has to design and implement
8 its web services to function the same irrespective of the browser one uses. (*Id.*)

9 Similarly, Steven Ganem, Group Product Manager for Google Analytics, testified that
10 Google Analytics' collection of one's data does not differ based on the browser one uses because
11 the whole purpose of data analytics is to measure the use of one's product and such measurement
12 must be collected and measured the same across different browsers so that the information is not
13 biased. (*Id.* at 157:5-158:19.) Thus, Google's javascript code needs to be identical for every
14 browser. (*Id.*) Dr. Adriene Felt, Director of Engineering for the Chrome Data Science &
15 Engineering team at Google, concurred. (*Id.* at 173:12-177:21.) Dr. Felt also explained that the
16 only data that is specific to Chrome is the X-client-header, which Google uses to conduct trial
17 periods on select browsers before rolling out certain features to all browsers. (*Id.* at 178:8-11,
18 180:1-20.)

19 Thus, the Court finds the undisputed evidence shows that the at-issue collection is
20 browser-agnostic, with the exception of the X-client-data header.

21 **C. Analysis of Relevant Policy Agreements**

22 Because the Court finds that the at-issue data collected is not specific to Chrome but
23 browser agnostic, the Court also finds that Google's general policies apply. More specifically, the
24 General Privacy Policy, New Account Creation Agreement, and Consent Bump Agreement
25 governs the collection of those categories of information identified by plaintiffs, namely "unique,
26 persistent cookie identifiers"; "users' browsing history in the form of the users' GET requests and
27 information relating to the substance, purport, or meaning of the website's portion of the
28 communication with the user"; "the contents of the users' POST communications"; and the "user

IP address and User-Agent information about their device.”

However, with respect to the X-client-data header, that data is specific to Chrome, and accordingly, the Chrome Privacy Notice governs the collection of that piece of data.⁷

D. Plaintiff-Specific Consent

Having identified the controlling agreement for each category of data collected, the Court analyzes (1) whether each named plaintiff consented to the at-issue conduct and (2) the extent to which the consents were effective and legally sufficient. This includes consenting to (a) the General Privacy Policy, (b) the Consent Bump Agreement, (c) the New Account Agreement, and (d) the Chrome Privacy Notice.

1. Evidence of Each Plaintiff’s Consent

a. General Privacy Policy (All Plaintiffs)

The undisputed evidence demonstrates that all plaintiffs are Google account holders and thereby agreed to Google’s General Privacy Policy when they created their Google accounts. (Fair Decl., ¶¶ 34-35; *see also* Dkt. No. 395-4, Stephen Broome Decl., Ex. 5, at Response 1B.) It is also undisputed that the material terms of the General Privacy Policy, at least until March 31, 2020, were the same throughout the class period. (FAC ¶ 34; Compl. Exs., at Exs. 7-16.)

The General Privacy Policy discloses that Google collects the at-issue data when users visit websites that use Google services. (Compl. Exs., at Ex. 7.) The policy states that Google collects “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.” (*Id.*) The

⁷ This makes sense given that browser settings are ever-changing and default settings have evolved over time. Some browsers may send more information to Google, and some send less, the amount varies depending on various settings. That is why it is important to describe the collection in browser agnostic terms like Google does in its general policies because, as shown at the evidentiary hearing, the settings and changes across browsers evolve over time, and at different times.

So, having Google’s disclosure of the at-issue data in browser-agnostic terms, rather than by specific-browser, enables Google users, irrespective of the browser used, to know how it is that Google collects and utilizes one’s data. Having this collection disclosed in Chrome’s Privacy Notice, as plaintiffs suggest, could create the impression that this collection only occurs on Chrome and not on other browsers.

1 policy explains that such information includes “search queries”; “Internet protocol address”;
2 “cookies”; and “referrer URL”. (*Id.*)

3 The General Privacy Policy also discloses how Google uses the at-issue data. (*Id.*) For
4 instance, Google discloses that the information collected “from all of [Google’s] services [is used]
5 to offer you tailored content—like giving you more relevant search results and ads.” (*Id.*)
6 Plaintiffs allege that Google combines users’ personal information with other data for purposes of
7 targeted advertising. (*Id.*) However, the privacy policy discloses that Google “may combine
8 personal information from one service with information, including personal information, from
9 other Google services” and that one’s “activity on other sites and apps may be associated with
10 your personal information in order to improve Google’s services and the ads delivered by
11 Google.” (*Id.*)

12 Plaintiffs also allege that Google engages in what plaintiff calls “cookie-syncing,” whereby
13 Google takes information from first party cookies and links it with Google’s own third party
14 cookies. (*Id.*) The General Privacy Policy also discloses this conduct under a paragraph titled
15 “linked with information about visits to multiple sites.” (*Id.*) The paragraph explains how “Google
16 Analytics is based on first-party cookies” and that data generated through Google Analytics “can
17 be linked, by the Google Analytics customer or by Google,” “to third party cookies.” (*Id.*) The
18 paragraph also explains that this information is used for targeted advertising. (*Id.*)

19 Thus, in agreeing to Google’s General Privacy Policy, the Court finds plaintiffs agreed to
20 the alleged data-collection (except for X-Client-data header) and the alleged use of the data.

21 *b. Consent Bump Agreement (Plaintiffs Crespo, Henry, Wilson, and*
22 *Johnson)*

23 The undisputed evidence demonstrates that plaintiffs Crespo, Henry, Wilson, and Johnson
24 consented to Google’s Consent Bump Agreement. Thus:

25 Crespo viewed the Consent Bump Agreement and selected the “I AGREE” button on
26 August 26, 2016. (Fair Decl., at Ex. 5.) Plaintiff Henry viewed the Consent Bump Agreement and
27 selected “I AGREE” on October 28, 2016. (*Id.* at Ex. 9.) Plaintiff Wilson viewed the Consent
28 Bump Agreement and selected “I AGREE” on December 13, 2018. (*Id.* at Ex. 12.) Plaintiff
Johnson viewed the Consent Bump Agreement on July 13, 2016, August 30, 2016, and October 9,

2017, respectively, and selected “I AGREE” each time. (*Id.* at Exs. 19-21.)

The Consent Bump Agreement, which did not materially change throughout the relevant class period, disclosed that users generate data when they use Google’s services, including “browsing data from Chrome and activity from sites and apps that partner with Google, including those that show ads from Google”; that “Google will use this information to make ads across the web more relevant”; “with this change, this setting will also let Google use data in your account to improve the relevance of ads that appear in Google products”; and that the settings “apply across all of your signed in devices and across all Google services.” (*Id.* at Ex. 6.) The Bump Agreement’s Learn More page also disclosed that other applications and services use Google technologies such as AdSense or Google Analytics and that as users use sites that use Google’s services, “your web browser may send certain information to Google that may include the web address of the page you’re visiting, your IP address, or cookies previously set by the site or Google. (*Id.* at Ex. 3 at GOOG-CABR-04067841.) The language right before the “I AGREE” button stated: “Choose I AGREE to turn these features on or MORE OPTIONS for more choices.” (*Id.* at GOOG-CABR-04067836.) Plaintiffs Crespo, Henry, Wilson, and Johnson all clicked “I AGREE” and thus consented to the collection of their browsing history, cookie identifiers, and IP address when they agreed to the Consent Bump Agreement.

c. *New Account Creation Agreement (Plaintiffs Calhoun, Wilson, Johnson, and Kindler)*

The undisputed evidence demonstrates that plaintiffs Calhoun, Wilson, Johnson, and Kindler agreed to Google’s New Account Creation Agreement when they created new Google accounts after June 2016. Thus:

Plaintiff Calhoun viewed and agreed to the New Account Creation Agreement on January 12, 2017 and June 24, 2017. (Fair Decl., Exs. 27-28.) Similarly, plaintiffs Wilson and Johnson also viewed and agreed to Google’s New Account Creation Agreement when they created new Google accounts on September 25, 2018 and September 9, 2019, respectively. (*Id.* at Exs. 38, 35.) Plaintiff Kindler viewed and agreed to Google’s New Account Creation Agreement on May 5, 2020 when she created a Google account on that date. (*Id.* at Ex. 32.)

During the class period, the New Account Agreement disclosed the type of data that is

collected when one uses a Google service, including “device IDs, IP addresses, cookie data, and location”; that such information is collected and used when one uses “apps or sites that use Google services like ads and Analytics”; that this is used to “deliver personalized ads, both on Google services and on sites and apps that partner with Google”; that it is also used to “conduct analytics and measurements”; and that Google “combine[s] data among our services and across your devices” for targeted advertising. (*Id.* at Ex. 3, at GOOG-CABR-04067829-30.) Thus, when plaintiffs clicked the “I AGREE” button they consented to the alleged data collection and conduct.

d. Chrome Privacy Notice (All Plaintiffs)

Similarly, it is undisputed that all plaintiffs agreed to the Chrome Privacy Notice. (Stephen Broome Decl., Ex. 5, at Response 1B.) The Chrome Privacy Notice, which applies to “features specific to Chrome,” discloses Google’s use and of the X-Client-data header. (Compl. Exs at Ex. 33.)

The Chrome Privacy Notice discloses just that:

Identifiers in Chrome

Chrome includes a number of unique and non-unique identifiers necessary to power features and functional services. . . . Where possible, we use non-unique identifiers and remove identifiers when they are no longer needed. Additionally, the following identifiers help us develop, distribute, and promote Chrome, but are not directly related to a Chrome feature.

- [. . .]
- [. . .]
- **Field trials.** We sometimes conduct limited tests of new features. Chrome includes a seed number that is randomly selected on first run to assign browsers to experiment groups. Experiments may also be limited by country (determined by your IP address), operating system, Chrome version, and other parameters. A list of field trials that are currently active on your installation of Chrome is included in all requests sent to Google. [Learn More](#).

(*Id.*) Clicking “Learn More” takes users to the Chrome Privacy Whitepaper which also describes the X-Client-data header. Accordingly, plaintiffs agreed to Google’s use of the X-Client-header data when they agreed to the Chrome Privacy Notice.

///

1 **2. Whether the Consent is Legally Sufficient⁸**

2 a. Analysis

3 Having determined that all plaintiffs have consented at least once, and for plaintiffs Wilson
4 and Johnson twice, to the collection of the at-issue data, plaintiffs make the alternative argument
5 that the consent was not effective or legally sufficient. For the reasons set forth below, the Court
6 disagrees.

7 The Ninth Circuit’s unpublished decision *Smith v. Facebook, Inc.*, 745 F. App’x 8-9 (9th
8 Cir. 2018) (affirming dismissal) is instructive. There the district court reviewed Facebook’s Terms
9 and Policies, which stated that Facebook “collect[s] information when you visit or use third party
10 websites and apps that use our Services” and that “we use all of the information we have about
11 you to show you relevant ads” and found that agreeing to such disclosures was “[k]nowing
12 authorization.” The court found that plaintiffs had consented to the alleged conduct and found that
13 “a reasonable person viewing those disclosures would understand that Facebook maintains the
14 practices of (a) collecting its users’ data from third-party sites and (b) later using the data for
15 advertising purposes.” *Smith v. Facebook*, 745 F. App’x at 8-9.

16
17 ⁸ Preliminarily, the parties dispute whether the Court may consider Google’s express
18 consent argument in light of Judge Koh’s prior ruling at the motion to dismiss stage. Plaintiffs
19 urge that Judge Koh’s prior ruling on Google’s motion to dismiss precludes the Court from
20 determining whether plaintiffs consented to the alleged conduct at summary judgment based on
21 the law of the case doctrine. Plaintiffs do not persuade. A ruling by a court for purposes of a
22 motion to dismiss does not bind the court on a subsequent motion for summary judgment as the
23 standards are entirely different: one considers plausibility, the other, the actual factual record. *See*
24 *e.g.*, *Braden Partners, LP v. Twin City Fire Ins. Company*, No. 14-cv-1689- JST, 2017 WL 63019,
25 at * 6 (N.D. Cal Jan. 5, 2017) (“Given the different standards for motions to dismiss and motions
26 for summary judgment, courts may (and routinely do) reconsider the same legal arguments at the
27 summary judgement stage) (citations omitted); *see also Peralta v. Dillard*, 744 F.3d 1076, 1088
28 (9th Cir. 2014), *cert denied*, 135 S. Ct. 946 (2015) (“Pretrial rulings, often based on incomplete
information, don’t bind district judges for the remainder of the case.”) Motions to dismiss are
bound by the pleadings. Judge Koh’s ruling did not consider all the disclosures that Google
proffers on summary judgment. Further, part of Judge Koh’s ruling was based on the proposition
that the General Privacy Policy was excluded from Google’s Terms of Service as of March 31,
2020. However, the undisputed evidence demonstrates that all plaintiffs agreed to Google’s
General Privacy Policy prior to March 31, 2020. Accordingly, the Court finds that it may therefore
consider Google’s express consent argument on summary judgment.

As applied here, the General Privacy Policy, Consent Bump Agreement, and New Account Agreement all have language that presents a similar level of specificity as Facebook’s disclosure. The General Privacy Policy discloses that Google collects “information about the services that you use and how you use them” as well as information when a user “visits a website that uses [Google’s] advertising services, or [when you] view and interact with our ads and content.” (Compl. Exs., at Ex. 7.) The Consent Bump Agreement disclosed that clicking “I AGREE” meant agreeing to allow Google to collect “activity from sites and apps that partner with Google, including those that show ads from Google.” (Fair Decl., at Ex. 3, at GOOG-CABR-04067836.) Similarly, the New Account Agreement also discloses that Google processes the at-issue data “when you use apps or sites that use Google’s services like ads, Analytics, and the YouTube video player” in part to “[d]eliver personalized ads . . . both on Google services and on sites and apps that partner with Google.” (*Id.* at Ex. 3, at GOOG-CABR-04067829-30.)

As in *Smith*, the Court finds that a reasonable person viewing those disclosures would understand that Google maintains the practices of (a) collecting its users’ data when users use Google services or third party sites that use Google’s services and (b) that Google uses the data for advertising purposes. The Court also finds that a reasonable user reviewing these same disclosures would understand that Google combines and links this information across sites and services for targeted advertising purposes. Likewise, in reviewing Google’s General Privacy Policy, a reasonable user would understand that Google engages in “cookie-syncing.”

b. Plaintiffs’ Additional Arguments

Plaintiffs proffer a set of six arguments in attempt to create a factual dispute as to whether plaintiffs consented to the alleged conduct. The Court addresses each. In general, the arguments repeat the notion that the disclosures were not specific enough and also posit that any consent is negated by the Chrome Privacy Notice and internal Google documents. None of these arguments persuade.

First, with respect to the assertion that the General Privacy Policy, Consent Bump Agreement, and New Account Agreement do not disclose the conduct at issue, nor the express promises at issue, plaintiffs fail to persuade for the reasons set forth above. (*See supra* sections

III.D.1-2a.) Rather than address the express language in these policies, plaintiffs largely ignore the text and cherry pick language to try and manufacture a factual dispute. Such attempt fails.

Second, plaintiffs argue that any consent under the Consent Bump Agreement is ineffective because the agreement does not give users the option to say “No.” The Court disagrees. The Consent Bump Agreement gives users two options: to either click “I AGREE” or “More Options”. (Fair Decl., ¶¶ 19, 24.) Users who clicked on the “More Options” were taken to a screen that allowed them to select either: “No changes – continue on your way”; “No changes – review key privacy settings more fully”; or “yes, I’m in – turn on these features.” (*Id.* at ¶ 24.) Thus, users had the option to decline the additional features.⁹

Third, plaintiffs also contend that the Consent Bump Agreement does not state that it overrides express promises made to Chrome users. Thus, according to plaintiffs, a user reading the Consent Bump Agreement may think that it does not apply to Chrome users. However, plaintiffs ignore the express language indicating that the settings, if turned on, “apply across all of your signed-in devices and across all Google services.” (*Id.* at ¶ 19.)

Fourth, plaintiffs aver that “the extent and scope of Google’s actual collection and use grossly exceed the scope of conduct disclosed.” (Dkt. No. 461-4, Opposition to Motion for Summary Judgment, (“Opp.”) at 2.) Importantly, this conduct is not alleged in, nor forms the basis of, plaintiffs’ operative complaint¹⁰ which only alleges that Google allegedly engages in “cookie-

⁹ Oddly, plaintiffs also submit that the Consent Bump Agreement “did not even garner consent for non-Chrome users” (Opp. at 8). This argument is irrelevant because plaintiffs seek to represent a class of Chrome users, not non-Chrome users.

¹⁰ For instance, plaintiffs argue that Google’s conduct exceeds its disclosures because Chrome sends more personal information to Google than other browsers, Google utilizes internal systems to sync and link data across services and sites, Google does not anonymize not-synced data, and that Google sells users’ personal information. (Opp. at 10-12.) However, none of this conduct is alleged to in the FAC. Rather, the FAC only focuses on Google’s receipt of the at-issue data, Google’s alleged creation of users’ profiles, and the conduct that plaintiffs call cookie-syncing or cookie decorator. (FAC ¶¶ 69, 141, 174, 180, 186, 258.) Thus, the Court does not address these new theories at summary judgment. *See Ray v. State Farm Mut. Auto. Ins. Co.*, 2021 WL 4902357, at *1 (9th Cir. Oct. 21, 2021) (explaining that “it was improper for the [plaintiffs] to advance these new theories for the first time in its opposition to summary judgment.”)

1 syncing”¹¹ and the practice of combining users’ information to create profiles for targeted
2 advertising.¹² Each is disclosed. A material dispute of fact on this topic does not exist.

3 Fifth, plaintiffs claim that any consent is negated by their acceptance of the Chrome
4 Privacy Notice. Plaintiffs argue that a reasonable user reading the Chrome Privacy Notice would
5 think that Google blocks all collection of the at-issue data when one uses the Chrome browser.
6 Specifically, plaintiffs focus on the statements that one “do[esn’t] need to provide any personal
7 information to use Chrome” and that “the personal information that Chrome stores won’t be sent
8 to Google unless you choose to store that data in your Google Account by turning on sync.”

9 To make this argument plaintiffs completely ignore critical text and read others out of
10 context. Importantly, the Chrome Privacy Notice explicitly indicates that it only “describes
11 features that are specific to Chrome.” The notice then explains that certain information is
12 automatically collected when people visit Google sites while using Chrome. The information
13 includes “web request, Internet Protocol address, browser type, browser language, the date and
14 time of your request and one or more cookies that may uniquely identify your browser.” The
15 notice also discloses that Chrome collects the requested URL, including the search query. Right
16 under this disclosure is a “More Information” section that states that “information that Google
17 receives when you used Chrome is used and protected under the Google Privacy Policy.” The
18 Privacy Policy is hyperlinked in this text. Much of this information constitutes the at-issue data in
19 this case. The Chrome Privacy Notice explains that personal information is not required to use
20

21 ¹¹ Plaintiffs describe “cookie-syncing” as the process whereby first-party cookies pass on
22 information that is gathered from its website to Google Analytics and Google then takes that
23 information and links it to Google’s own third party cookies. (FAC ¶ 69.) In this regard, the
24 General Privacy Policy discloses this conduct under a paragraph titled “linked with information
25 about visits to multiple sites.” The paragraph explains how “Google Analytics is based on first-
26 party cookies” and that data generated through Google Analytics “can be linked, by the Google
27 Analytics customer or by Google,” “to third party cookies.” The General Privacy Policy also
28 discloses that this information is used for targeted advertising.

¹² Similarly, Google discloses that it may combine users’ personal information across
Google services and that one’s activity on other sites may be associated with other personal
information in Google’s possession for targeted advertising. Plaintiffs’ arguments that Google did
not disclose the amount of data, or the technological way in which the data is collected, does not
persuade. Google discloses that it collects the at-issue data, that the data may be combined and
linked with other data from different sources, and that the combined data may be used for targeted
advertising.

1 Chrome, but when one uses Chrome and provides personal information, that information is
2 collected in accordance with Google's General Privacy Policy.

3 Further, plaintiffs contend that a dispute regarding consent also exists because the Chrome
4 Privacy Notice provides that "the personal information that Chrome stores won't be sent to
5 Google unless you choose to store that data in your Google Account by turning on sync."
6 According to plaintiffs, Google breaches this promise by receiving Chrome users' data. Again,
7 plaintiffs ignore that the Notice also explains that Chrome "stores information locally on your
8 system" when using the basic browser mode. The information might include: "browsing history
9 information" such as "the URLs of pages that you visit, a cache of text, images, and other
10 resources from those pages" and in some instances "a list of some of the IP addresses linked from
11 those pages." However, plaintiffs have not established that the at-issue data collection is
12 information that Chrome stores. Rather, the at-issue data here is data that Google receives when
13 users visit websites that utilize Google services while using Chrome. Thus, Google's promise not
14 to store information does not establish a triable issue of fact.

15 Thus, the statements in the Chrome Privacy Notice cannot be read in a vacuum or cherry-
16 picked. Nor can express language be ignored. As explained above, the at-issue data is not specific
17 to Chrome, nor is the alleged misuse of such information. (*See supra* section III.B.) Consent is not
18 negated. Plaintiffs' interpretation is belied by the express language of the Chrome Privacy Notice.
19 Accordingly, plaintiffs' argument that the Chrome Privacy Notice negates any alleged consent
20 also fails.

21 Finally, plaintiffs submit that any supposed consent is negated because documents suggest
22 Google admits that its consent model is broken and does not live up to the express promises.
23 Here, plaintiffs identify various internal documents by Google employees that comment on
24 Google's practices. The documents fail to establish a triable issue of fact as to whether plaintiffs
25 consented to the at-issue conduct at least three reasons.

26 One: many of the documents are general in nature and do not address the specific
27 disclosures and/or at-issue data. (Barnes Decl., Exs. 24, 47, 61) (untitled and undated draft
28 documents explaining Google's plans and vision for future disclosures and commenting on the

1 state of Google’s current consent flow)¹³; *see also id.* at Ex. 59 (document answering the question
2 “What is Google’s perspective on the use of encrypted PII (i.e. email) for user tracking
3 generally?”); *id.* at Ex. 60-428 (plaintiffs refer to subsection titled “Apple/ Firefox changes [3P
4 Cookies Removed] Don’t Change the User Experience”).

5 Two: plaintiffs misquote and cherry-pick. For instance, plaintiffs cite Exhibit 53 for the
6 proposition that “[f]or signed-in users, Googlers internally admit ‘there’s no real difference’
7 between Sync and Signed in But Not Consent for Sync ‘for users who’d prefer not to store their
8 data with Google.’” However, the context of the email is relevant. The sender of the email
9 explained that they are left wondering whether “there [is] really a need for Sync in the longer
10 term” because “[b]oth Sign-in and Sync are tied to one’s Google account, so there’s no real
11 difference there for users who’d prefer not to store data with Google.” Similarly, plaintiffs cite
12 Exhibit 52 for the proposition that Google admits that users would be shocked to learn that we’re
13 still gathering info about them[.]” However, plaintiffs omit both the beginning and the end of the
14 sentence which indicate that the comment was based on the speaker’s suspicion (“I suspect”) and
15 the speaker’s acknowledgement that they could be mistaken (“but perhaps I’m wrong”); *see also*
16 *id.* at Ex. 51 (plaintiffs proffer as stating that “apart from David [Monsees], nobody can answer”
17 the question of what “data is being collected (or not) [.]” Plaintiffs omit the response email which
18 followed stating, “I don’t think we expect people to know what data exactly is being collected but
19 I hope people can understand that we are still collecting data within in app if they say ‘no’ to the
20 cross-product consent [] and that we are also collecting data in all other apps”); *id.* at Ex. 15
21 (“Well, we know from research . . . that users generally have no idea what they’re agreeing to
22 *because of this automatic scroll-n-click behaviors*” not “we know from research . . . that users
23 generally have no idea what they’re agreeing to”) (emphasis supplied).

24 Three: Plaintiffs mischaracterize key deposition testimony. For instance, plaintiffs claim
25 Abdelkarim Mardini’s, Google’s Head of Chrome Trust & Safety, “admitted last month under

26
27 ¹³ Plaintiffs rely on many draft documents that are either undated, untitled, or do not have
28 an author/drafter listed and thus, cannot, without more, be attributed to Google as admissions.
Even viewing the documents in favor of plaintiffs, they fail to establish a genuine material factual
dispute for the reasons identified herein.

oath that he was not even aware Chrome sent PI when not synced.” (*Id.* at Ex. 1 at 47:22-53:4; 54:2-8). Plaintiffs’ summary is inaccurate. Rather, Mr. Mardini testified that when visiting a non-Google site using a Chrome browser, the X-client-data header could potentially be sent back to Google if the header is available on that browser. Plaintiffs allege that the X-client-data header is personal information, thus plaintiffs’ representation that Mr. Mardini did not know that Chrome sent personal information when not synced is not true. Moreover, he does not mention one’s sync status.

In light of the foregoing, the documents plaintiffs cite, viewed individually and holistically, are insufficient to establish a genuine material dispute as to whether plaintiffs consented to Google’s conduct.

Thus, based on the record, the Court concludes, as a matter of law that Google adequately disclosed, and plaintiffs consented to, the collection of the at-issue data. Accordingly, Google’s motion for summary judgment based on consent is hereby **GRANTED**.


IV. CONCLUSION

For the foregoing reasons, the Court hereby **GRANT** Google’s Motion for Summary Judgment. The Court **DENIES** plaintiffs’ Motion for Class Certification and plaintiffs’ Motion for Leave to Supplement the Briefing Regarding Remedies **AS MOOT**. The Court **DENIES** plaintiffs’ Motion for Leave to Supplement the Record as to Google’s Motion for Summary Judgment and to File a Sur-Reply. The parties’ pending motions to seal will be addressed by separate court order.

This Order terminates Docket Numbers 340, 395, 425, 427, 488, 855, and 909.

IT IS SO ORDERED.

Dated: December 12, 2022


YVONNE GONZALEZ ROGERS
UNITED STATES DISTRICT COURT JUDGE

Appendix A

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Some new features for your Google Account

We've introduced some optional features for your account, giving you more control over the data Google collects and how it's used, while allowing Google to show you more relevant ads.

What changes if you turn on these new features?

1. More information will be available in your Google Account, making it easier for you to review and control

When you use Google services like Search and YouTube, you generate data — things like what you've searched for and videos you've watched. You can find and control that data in *My Account* under the **Web & App Activity** setting.

With this change, this setting may also include browsing data from Chrome and activity from sites and apps that partner with Google, including those that show ads from Google.

You have Chrome browsing history stored in your Google Account. [Learn more](#) about how turning on this setting affects how this data is used for personalization.

2. Google will use this information to make ads across the web more relevant for you

In *My Account*, the **Ads Personalization** setting currently lets Google use data in your account to tailor ads that appear in Google products.

With this change, this setting will also let Google use data in your account to improve the relevance of ads on websites and apps that partner with Google.

These settings apply across all of your signed-in devices and across all Google services. You can change them any time in *My Account*. [Learn more](#) about these features, including how they affect shared devices.

What's still the same?

- Google does not sell your personal information to anyone
- You control the types of information we collect and use at *My Account* (myaccount.google.com)

Choose **I AGREE** to turn these features on or **MORE OPTIONS** for more choices.

[MORE OPTIONS](#) [I AGREE](#)

(Fair Decl., at Ex. 3, at GOOG-CABR-04067836.)

Appendix B

Privacy and Terms

By choosing "I agree" below you agree to Google's [Terms of Service](#).

You also agree to our [Privacy Policy](#), which describes how we process your information, including these key points:

Data we process when you use Google

- When you use Google services to do things like write a message in Gmail or comment on a YouTube video, we store the information you create.
- When you search for a restaurant on Google Maps or watch a video on YouTube, for example, we process information about that activity – including information like the video you watched, device IDs, IP addresses, cookie data, and location.
- We also process the kinds of information described above when you use apps or sites that use Google services like ads, Analytics, and the YouTube video player.

Depending on your account settings, some of this data may be associated with your Google Account and we treat this data as personal information. You can control how we collect and use this data at My Account (myaccount.google.com).

Why we process it

We process this data for the purposes described in [our policy](#), including to:

- Help our services deliver more useful, customized content such as more relevant search results;
- Improve the quality of our services and develop new ones;
- Deliver personalized ads, both on Google services and on sites and apps that partner with Google;
- Improve security by protecting against fraud and abuse; and
- Conduct analytics and measurement to understand how our services are used.

Combining data

We also combine data among our services and across your devices for these purposes. For example, we show you ads based on information from your use of Search and Gmail, and we use data from trillions of search queries to build spell-correction models that we use across all of our services.

CANCEL I AGREE

(*Id.* at GOOG-CABR-04067829-30.)