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.

> When you use our services or view content provided by Google, we automatically collect and store certain information in server logs, [including] 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 [and] cookies that may uniquely identify your browser or your Google Account.

Id. Subsequent versions of Google's Privacy Policy made similar disclosures.

Starting on May 25, 2018, Google's Privacy Policy made statements regarding Chrome's Incognito Mode:

> You can use our services in a variety of ways to manage your privacy. For example, you can sign up for a Google Account if you want to create and manage content like email or photos, or see more relevant search results. . . . You can also choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

Schapiro Decl. Exh. 8. Subsequent versions of Google's Privacy Policy made similar statements.

Second, Google's Chrome Privacy Notice dated June 21, 2016 also made statements regarding Chrome's Incognito Mode:

> You can limit the information Chrome stores on your system by using incognito mode or guest mode. In these modes, Chrome won't store certain information, such as:
>
> - Basic browsing history information like URLs, cached paged text, or IP addresses of pages linked from the websites you visit.
> - Snapshots of pages that you visit . . . .
>
> How Chrome handles your incognito or guest information
>
> Cookies. Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new cookies on your system while you are in these modes, but they'll only be stored and transmitted until you close the incognito or guest window.

Schapiro Decl. Exh. 17.

Third, Google's webpage entitled "Search & browse privately" makes the following statements regarding private browsing:

> You're in control of what information you share with Google when you search. To browse the web privately, you can use private

> browsing, sign out of your account, change your custom results settings, or delete past activity.
>
> If you want to search the web without saving your search activity to your account, you can use private browsing mode in a browser (like Chrome or Safari).
>
> How private browsing works
>
> Private browsing works differently depending on which browser you use. Browsing in private usually means:
>
> - The searches you do or sites you visit won't be saved to your device or browsing history.
> - Files you download or bookmarks you create might be kept on your device.
> - Cookies are deleted after you close your private browsing window or tab.
> - You might see search results and suggestions based on your location or other searches you've done during your current browsing session.

Schapiro Decl. Exh. 18.

Fourth, Google's webpage entitled "How private browsing works in Chrome" makes the following statements regarding private browsing:

> When you browse privately, other people who use the device won't see your history . . . Cookies and site data are remembered while you're browsing, but deleted when you exit Incognito mode.
>
> Your activity might still be visible.
>
> Incognito mode stops Chrome from saving your browsing activity to your local history. Your activity . . . might still be visible to:
>
> - Websites you visit, including the ads and resources used on those sites
> - Websites you sign in to
> - Your employer, school, or whoever runs the network you're using
> - Your internet service provider
> - Search engines

- Search engines may show search suggestions based on your location or activity in your current Incognito browsing session.

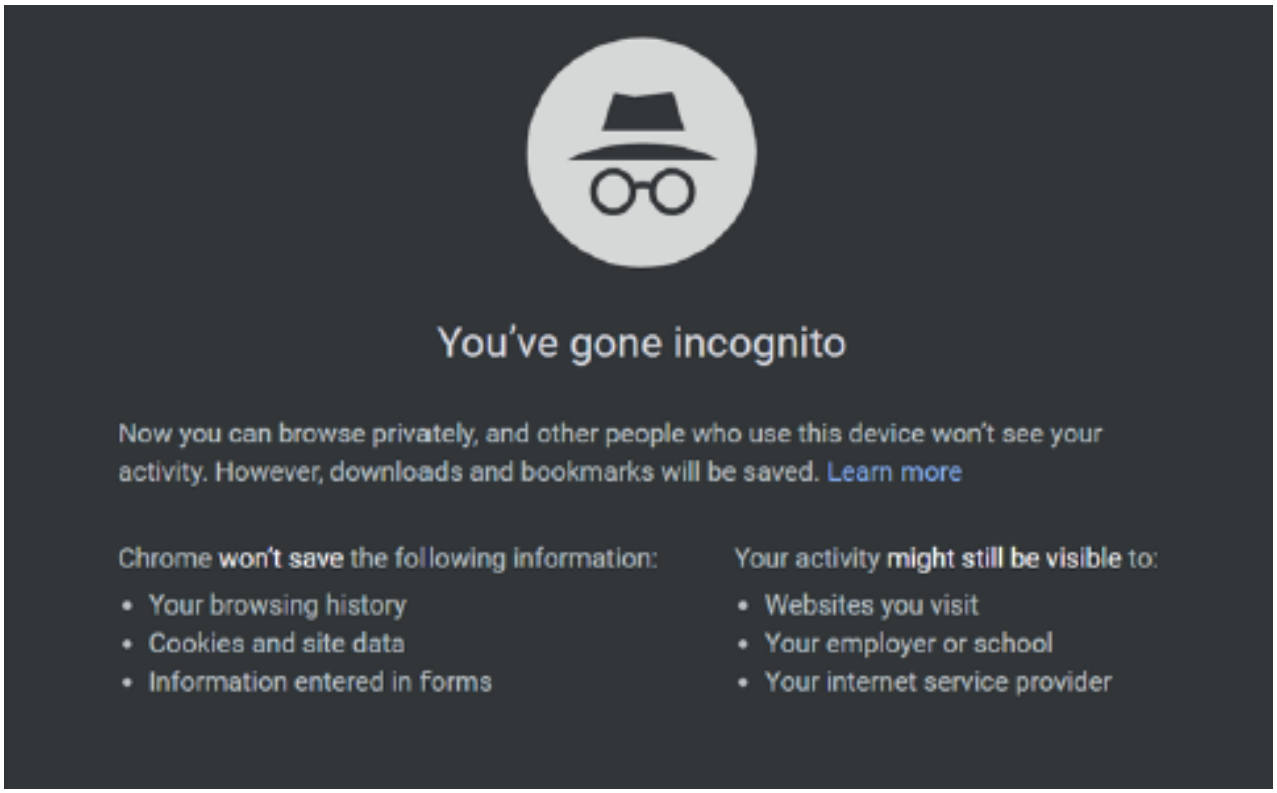
Some of your info might still be visible.

A web service, website, search engine, or provider may be able to see:

- Your IP address, which can be used to identify your general location
- Your activity when you use a web service . . . .

Schapiro Decl. Exh. 19.

Fifth, when a user enables Incognito Mode in the Chrome Browser, the following "Splash Screen" is displayed to the user with similar statements regarding private browsing mode:



FAC ¶ 52.

Finally, Plaintiffs' complaint alleges that Google and its officials made additional statements regarding private browsing. For instance, Plaintiffs allege that, on September 27, 2016, Google's Director of Product Management Unni Narayana published an article in which he

explained that Google was giving users "more control with incognito mode." FAC ¶ 146. The article stated the following: "Your searches are your business . . . When you have incognito mode turned on in your settings, your search and browsing history will not be saved." *Id.* ¶¶ 42, 146. Moreover, Plaintiffs allege that, on May 7, 2019, the New York Times published an opinion article written by Google's CEO, Sudar Pichai, who explained that Google focuses on "features that make privacy a reality." *Id.* ¶ 146. The article stated: "For example, we recently brought Incognito mode, the popular feature in Chrome that lets you browse the web without linking any activity to you, to YouTube." *Id.*

B. Procedural History

On June 2, 2020, Plaintiffs filed the instant case against Alphabet, Inc. and Google LLC. ECF No. 1. Plaintiffs bring five claims: (1) unauthorized interception under the Wiretap Act, 18 U.S.C. § 2510 *et seq.*; (2) violation of the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 631 and 632; (3) violation of the California Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502; (4) invasion of privacy; and (5) intrusion upon seclusion. FAC ¶¶ 202–266.

Plaintiffs seek to represent two classes: (1) "All Android device owners who accessed a website containing Google Analytics or Ad Manager using such a device and who were (a) in "private browsing mode" on that device's browser and (b) were not logged into their Google account on that device's browser, but whose communications, including identifying information and online browsing history, Google nevertheless intercepted, received, or collected from June 1, 2016 through the present" and (2) "All individuals with a Google account who accessed a website containing Google Analytics or Ad Manager using any non-Android device and who were (a) in "private browsing mode" in that device's browser, and (b) were not logged into their Google account on that device's browser, but whose communications, including identifying information and online browsing history, Google nevertheless intercepted, received, or collected from June 1, 2016 through the present." *Id.* ¶ 192.

On August 20, 2020, Plaintiffs and Alphabet stipulated to voluntarily dismiss Alphabet from the case without prejudice. ECF No. 51. On August 24, 2020, the Court granted the stipulation and voluntarily dismissed Alphabet, leaving Google as the only defendant. ECF No. 57.

On August 20, 2020, Google filed a motion to dismiss the complaint. ECF No. 53. On September 21, 2020, Plaintiffs filed a first amended complaint in lieu of opposing the motion to dismiss. ECF No. 68. On October 6, 2020, the Court denied as moot the motion to dismiss. ECF No. 74.

On October 21, 2020, Google filed the instant motion to dismiss the first amended complaint, ECF No. 82 ("Mot.") and a request for judicial notice, ECF No. 84. On November 18, 2020, Plaintiffs filed an opposition to Google's motion, ECF No. 87 ("Opp'n"), a response to Google's request for judicial notice, ECF No. 88, and their own request for judicial notice, ECF No. 89. On December 7, 2020, Google filed a reply in support of its motion to dismiss, ECF No. 92 ("Reply"), and a response to Plaintiffs' response regarding Google's request for judicial notice, ECF No. 93.

The Court may take judicial notice of matters that are either "generally known within the trial court's territorial jurisdiction" or "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b). However, to the extent any facts in documents subject to judicial notice are subject to reasonable dispute, the Court will not take judicial notice of those facts. *See Lee v. City of Los Angeles*, 250 F.3d 668, 689 (9th Cir. 2001), *overruled on other grounds by Galbraith v. County of Santa Clara*, 307 F.3d 1119 (9th Cir. 2002).

Google requests that the Court take judicial notice of twenty-seven documents, which include Google's Terms of Service, fifteen versions of Google's Privacy Policy, two versions of Google's Chrome Privacy Notice, and nine publicly available Google webpages. ECF No. 84. Plaintiffs request that the Court take judicial notice of Google's Privacy Policy in effect between

March 31, 2020 and July 1, 2020, which is one of the fifteen versions of Google's Privacy Policy of which Google requests the Court take judicial notice. ECF No. 89. These documents appear on publicly available websites and are thus proper subjects for judicial notice. *See, e.g.*, *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 813–14 (N.D. Cal. 2020) (taking judicial notice of Google's Terms of Service, Privacy Policy, and a Google blog post); *Matera v. Google, Inc.*, 2016 WL 5339806, at *7 (N.D. Cal. Sept. 23, 2016) (taking judicial notice of Google's Terms of Service, "various versions of Google's Privacy Policy," and a Google webpage entitled "Updates: Privacy Policy").

Plaintiffs contend that, as to six of the webpages presented by Google (Exhibits 19, 20, 22, 23, 24, and 25 to the Schapiro Declaration), Google does not identify the dates on which they became publicly available, so the Court should take judicial notice of these webpages only as to their existence on the date the webpage was last accessed. ECF No. 88 at 1. However, Google demonstrates using the Internet Archive's "Wayback Machine" that Exhibits 19 and 20 have been publicly available since August 18, 2018, and substantively identical versions of Exhibits 22 to 25 have been publicly available since March 25, 2015 (Exhibit 22); June 13, 2014 (Exhibit 23); November 12, 2012 (Exhibit 24); and January 28, 2015 (Exhibit 25). ECF No. 93 at 3–4. "Courts have taken judicial notice of the contents of web pages available through the Wayback Machine as facts that can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." *See, e.g.*, *Erickson v. Nebraska Mach. Co.*, 2015 WL 4089849, at *1 n. 1 (N.D. Cal. July 6, 2015) (taking judicial notice of websites where "Plaintiffs provided copies of current versions of these websites . . . but the Internet Archive's Wayback Machine shows that the websites were substantively identical during the relevant timeframe"). Accordingly, the Court takes judicial notices of these webpages as of these dates. Thus, the Court GRANTS Google's request for judicial notice and GRANTS Plaintiffs' request for judicial notice.

Finally, at the hearing on the instant motion, Google raised for the first time arguments regarding the Court's website. *See* Tr. of Feb. 25, 2021 Hearing at 47:13–16, ECF No. 104. In its

decision on the instant motion, the Court will not consider Google's untimely arguments. *See In re Apple Inc. Securities Litigation*, 2011 WL 1877988, *5 n. 6 (N.D. Cal. May 17, 2011) ("The Court is not inclined to consider this argument given that it was not briefed but rather was raised for the first time at the end of the hearing"); *White v. FedEx Corp.*, 2006 WL 618591, *2 (N.D. Cal. Mar. 13, 2006) ("The Court will not consider any arguments or evidence raised for the first time at the hearing"). Accordingly, the Court DENIES Google's motion to file an additional reply regarding the Court's website, ECF No. 112.

II. LEGAL STANDARD

A. Dismissal Pursuant to Federal Rule of Civil Procedure 12(b)(6)

Rule 8(a) of the Federal Rules of Civil Procedure requires a complaint to include "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a). A complaint that fails to meet this standard may be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(6). Rule 8(a) requires a plaintiff to plead "enough facts to state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). "The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (internal quotation marks omitted). For purposes of ruling on a Rule 12(b)(6) motion, the Court "accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008).

The Court, however, need not accept as true allegations contradicted by judicially noticeable facts, *see Shwarz v. United States*, 234 F.3d 428, 435 (9th Cir. 2000), and it "may look beyond the plaintiff's complaint to matters of public record" without converting the Rule 12(b)(6) motion into a motion for summary judgment, *Shaw v. Hahn*, 56 F.3d 1128, 1129 n.1 (9th Cir. 1995). Nor must the Court "assume the truth of legal conclusions merely because they are cast in

the form of factual allegations." *Fayer v. Vaughn*, 649 F.3d 1061, 1064 (9th Cir. 2011) (per curiam) (quoting *W. Mining Council v. Watt*, 643 F.2d 618, 624 (9th Cir. 1981)). Mere "conclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss." *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004).

B. Leave to Amend

If the Court determines that a complaint should be dismissed, it must then decide whether to grant leave to amend. Under Rule 15(a) of the Federal Rules of Civil Procedure, leave to amend "shall be freely given when justice so requires," bearing in mind "the underlying purpose of Rule 15 to facilitate decisions on the merits, rather than on the pleadings or technicalities." *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (en banc) (alterations and internal quotation marks omitted). When dismissing a complaint for failure to state a claim, "'a district court should grant leave to amend even if no request to amend the pleading was made, unless it determines that the pleading could not possibly be cured by the allegation of other facts." *Id.* at 1130 (internal quotation marks omitted). Accordingly, leave to amend generally shall be denied only if allowing amendment would unduly prejudice the opposing party, cause undue delay, or be futile, or if the moving party has acted in bad faith. *Leadsinger, Inc. v. BMG Music Publ'g*, 512 F.3d 522, 532 (9th Cir. 2008).

III. DISCUSSION

In the instant motion, Google first contends that Plaintiffs' claims should be dismissed because Plaintiffs and the websites consented to Google's receipt of the data. Mot. at 9–13. Google later argues that Plaintiffs' claims should be dismissed under the statutes of limitations. *Id*. at 23–25. Google also argues that Plaintiffs have failed to state their claims for additional reasons. *Id*. at 13–23. The Court addresses in turn: (1) consent; (2) the statutes of limitations; and (3) Google's other arguments for dismissal.

A. Consent

Google contends that (1) all claims should be dismissed because Plaintiffs consented to

Google's receipt of the data, and (2) Plaintiffs' Wiretap Act claims should be dismissed because the websites consented to Google's receipt of the data. *Id.* at 9–13. The Court addresses each argument in turn.

1. Google has not shown that Plaintiffs consented.

Consent is a defense to Plaintiffs' claims. *See* 18 U.S.C. § 2511(2)(d) (Wiretap Act) (providing that it is not "unlawful . . . for a person . . . to intercept a[n] . . . electronic communication . . . where one of the parties to the communication has given prior consent to such interception"); Cal. Pen. Code §§ 631(a), 632(a) (CIPA) (prohibiting wiretapping and eavesdropping "without the consent of all parties to the communication"); Cal. Pen. Code § 502(c)(2) (CDAFA) (providing that a person who "knowingly accesses and without permission takes, copies, or makes use of any data" is guilty of a public offense); *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) ("Plaintiff's consent . . . bars their common-law tort claims and their claim for invasion of privacy under the California Constitution."). Accordingly, Google contends that Plaintiffs consented to Google's alleged data collection while they were in private browsing mode. Mot. at 10–11.

"[A]s 'the party seeking the benefit of the exception,' it is Google's burden to prove consent." *Matera v. Google Inc.*, 2016 WL 5339806, at *17. Consent "can be explicit or implied, but any consent must be actual." *In re Google, Inc.*, 2013 WL 5423918, at *12 (N.D. Cal. Sept. 26, 2013). In order for consent to be actual, the disclosures must "explicitly notify" users of the practice at issue. *Id.* 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). The disclosures must have only one plausible interpretation for a finding of consent. *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 794 (N.D. Cal. 2019). "[I]f a reasonable . . . user could have plausibly interpreted the contract language as not disclosing that [the defendant] would engage in particular conduct, then [the defendant] cannot obtain dismissal of a claim about that conduct (at least not

based on the issue of consent)." *Id.* at 789–90.

In the instant motion, Google contends that users expressly consented to Google's alleged data collection while they were in private browsing mode. Mot. at 10–11. In *In re Google, Inc.*, this Court rejected a similar argument made by Google. 2013 WL 5423918, at *12–*14. In that case, the plaintiffs alleged that Google had intercepted their email communications over Gmail, Google's email service, in order to create user profiles and provide targeted advertising. *Id*. at *1. In Google's motion to dismiss, Google contended that the plaintiffs expressly consented to the interception of their emails and pointed to its Terms of Service and Privacy Policies. *Id*. at *13. Analyzing these policies, the Court concluded that "[n]othing in the [p]olicies suggests that Google intercepts email communication in transit between users, and in fact, the policies obscure Google's intent to engage in such interceptions." *Id*. Accordingly, the Court found that "a reasonable Gmail user who read the Privacy Policies would not have necessarily understood that her emails were being intercepted to create user profiles or to provide targeted advertisements." *Id*.

The Court rejects Google's argument in the instant case for two reasons. First, Google cannot demonstrate that Plaintiffs expressly consented because Google did not notify users that it would be engaging in the alleged data collection while Plaintiffs were in private browsing mode. Second, as to Plaintiffs' Wiretap Act claim, consent is not a defense because Google allegedly intercepted Plaintiffs' communications for the purpose of violating other laws. The Court discusses each reason in turn.

First, Google cannot demonstrate that Google notified Plaintiffs that Google would engage in the alleged data collection while Plaintiffs were in private browsing mode. Google argues that Plaintiffs expressly consented to Google's Terms of Service, which incorporated Google's Privacy Policy, and Google's Privacy Policy disclosed that Google would receive the data from its third-party services. Mot. at 10–11. However, Google's Privacy Policy does not disclose Google's alleged data collection while Plaintiffs were in private browsing mode. Google's Privacy Policy provides:

> 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.
>
> When you use our services or view content provided by Google, we automatically collect and store certain information in server logs, [including] 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 [and] cookies that may uniquely identify your browser or your Google Account.

Schapiro Decl. Exh. 1. This general disclosure never mentions private browsing. Nor does it explain that Google collects this data from users in private browsing mode. Google's Privacy Policy states:

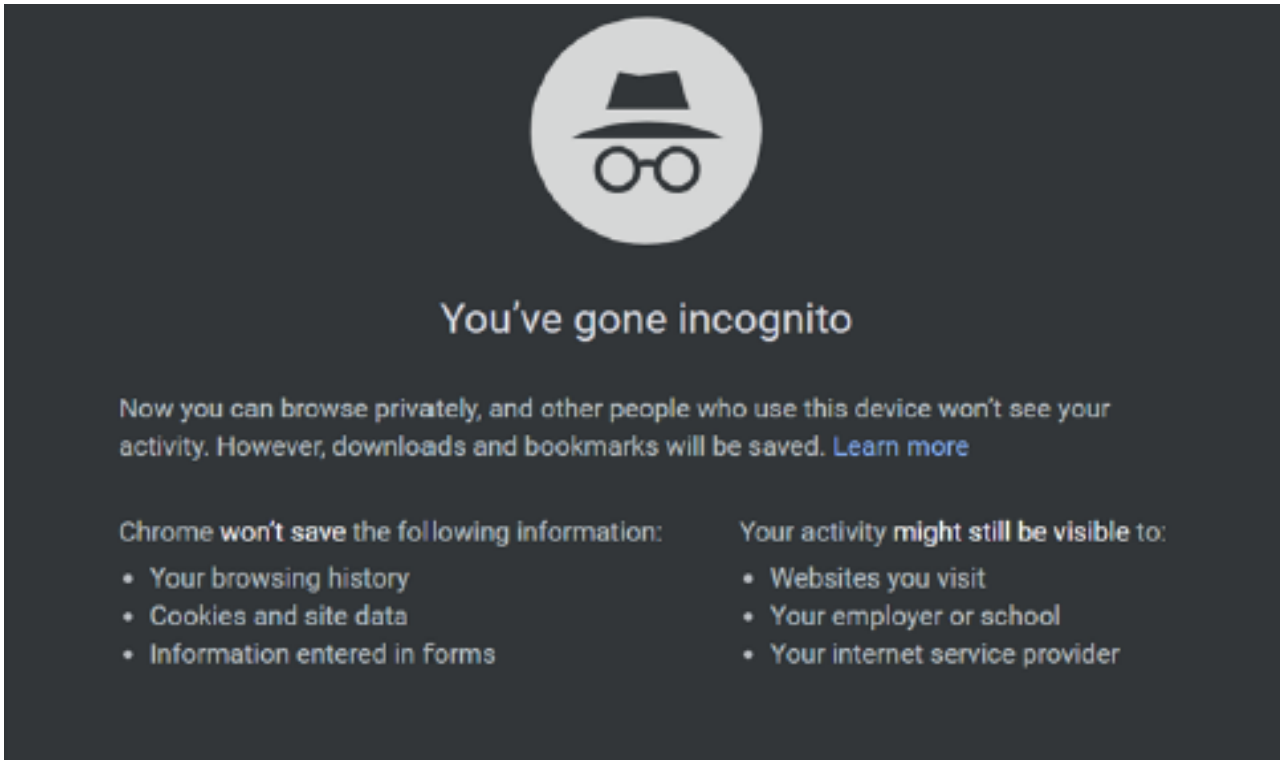
> Our Privacy Policy explains:
>
> - What information we collect and why we collect it.
> - How we use that information.
> - The choices we offer, including how to access and update information.

Id. Accordingly, a Google user reading the general disclosure above, which never mentions private browsing mode, might have reasonably concluded that Google does not collect this data from users in private browsing mode.

In addition to Google's failure to mention private browsing, Google's representations regarding private browsing present private browsing as a way that users can manage their privacy and omit Google as an entity that can view users' activity while in private browsing mode. The Court addresses in turn five documents that contain Google's representations regarding private browsing: (1) the Incognito Splash Screen; (2) the "How private browsing works in Chrome" webpage; (3) the "Search and browse privately" webpage; (4) the Chrome Privacy Notice; and (5) Google's Privacy Policy.

First, the Incognito Splash Screen appeared to every user each time they enabled Incognito

mode, immediately before they began their private browsing session:



The Incognito Splash Screen makes three relevant representations regarding private browsing mode. One, the Incognito Splash Screen omits Google from the list of entities that can view a user's activity in private browsing mode: "Your activity might still be visible to: Websites you visit[;] Your employer or school[;] Your internet service provider." FAC ¶ 52. Although the Splash Screen states that websites may be able to see a user's activity, the Splash Screen does not state that Google sees a user's activity. *Id*. Based on the omission of Google from the list of entities that can see a user's activity, a user might have reasonably concluded that Google would not see his or her activity. Moreover, the omission of Google from the list of entities "obscure[s] Google's intent to engage in such interceptions." 2013 WL 5423918, at *13.

Two, the Incognito Splash Screen states: "Now you can browse privately, and other people who use this device won't see your activity[.]" FAC ¶ 52. According to Google, this sentence clarifies that Incognito mode is about privacy from other users of the same device, not privacy

from Google. Specifically, Google reads the second phrase of this sentence ("other people who use this device won't see your activity") to provide more specification to the first phrase ("Now you can browse privately."). FAC ¶ 52. However, the Court concludes that a reasonable user could have read the two phrases as being independent of each other: "Now you can browse privately, *and* other people who use this device won't see your activity[.]" *Id*. (emphasis added). Accordingly, a reasonable user could have read this sentence to state that Incognito mode provided privacy from Google and privacy from other people who use the same device.

Three, the Incognito Splash Screen states "Chrome won't save . . . [y]our browsing history [or] [c]ookies and site data." *Id*. Google argues that this sentence is accurate because, when Google collects the alleged data, Chrome is not storing the data; rather, the user's browser is transmitting the data to Google's server. However, the Court concludes that a reasonable user could read this statement to mean that their browsing history and cookies and site data would not be saved. Moreover, the Court notes that a user might reasonably associate Chrome with Google because Chrome is Google's browser.

Second, like the Incognito Splash Screen, the Google webpage entitled "How private browsing works in Chrome" omits Google from the entities to which a user's private browsing activity may be visible. That webpage discloses that a user's private browsing activity might be visible to "websites [she] visit[s], *including the ads and resources used on those sites*." Schapiro Decl. Exh. 19 (emphasis added). However, this webpage never references Google.

Third, Google's webpage entitled "Search & browse privately" states: "You're in control of what information you share with Google when you search. To browse the web privately, you can use private browsing . . . ." Schapiro Decl. Exh. 18. However, Plaintiffs allege that, in reality, users are not in control of what information they share with Google when they use private browsing mode. Rather, Google engages in the alleged data collection regardless of whether users are in private browsing mode.

Fourth, Google's Chrome Privacy Notice dated June 21, 2016 similarly stated that: "You

can limit the information Chrome stores on your system by using incognito mode or guest mode. In these modes, Chrome won't store certain information, such as: . . . Basic browsing history information like URLs, cached paged text, or IP addresses of pages linked from the websites you visit [and] Snapshots of pages that you visit . . . ." Schapiro Decl. Exh. 17. As with the Incognito Splash Screen, a reasonable user could read this statement to mean that their browsing history and IP address would not be saved.

Fifth, since May 25, 2018, Google's Privacy Policy has presented Incognito mode as a way that users can control the information that Google collects: "You can use our services in a variety of ways to manage your privacy. For example, . . . You can . . . choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used." Schapiro Decl. Exh. 8. Google's Privacy Policy makes clear that "Our services include . . . Products that are integrated into third-party apps and sites, like ads . . . ." *Id*. However, Plaintiffs allege that, in reality, private browsing does not permit them to manage their privacy or control what Google collects because Google collects this information even when they use private browsing mode.

In addition, Plaintiffs' complaint alleges that Google and its officials made additional statements regarding private browsing. For instance, Plaintiffs allege that, on September 27, 2016, Google's Director of Product Management Unni Narayana published an article in which he explained that Google was giving users "more control with incognito mode." FAC ¶ 146. The article stated the following: "Your searches are your business . . . When you have incognito mode turned on in your settings, your search and browsing history will not be saved." *Id*. ¶¶ 42, 146. Moreover, Plaintiffs allege that, on May 7, 2019, the New York Times published an opinion article written by Google's CEO, Sudar Pichai, who explained that Google focuses on "features that make privacy a reality." *Id*. ¶ 146. The article stated: "For example, we recently brought Incognito mode, the popular feature in Chrome that lets you browse the web without linking any activity to you, to YouTube." *Id*. These statements suggest that a user's activity in private

browsing mode is not saved or linked to the user.

Reviewing these disclosures, the Court concludes that Google did not notify users that Google engages in the alleged data collection while the user is in private browsing mode. Accordingly, Google cannot show that Plaintiffs expressly consented to Google's collection of data while Plaintiffs were in private browsing mode. *See In re Google*, 2013 WL 5423918, at *13 (rejecting Google's argument that users expressly consented because Google did not notify users of the alleged interceptions).

Second, as to Plaintiffs' Wiretap Act claim, consent is not a defense where the "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. § 2511(2)(d). Under this exception, Plaintiffs must allege that either the "primary motivation or a determining factor in [the interceptor's] actions has been to injure plaintiffs tortiously." *In re Google Inc., Gmail Litig.*, 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014) (quoting *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 518 (S.D.N.Y. 2001)).

In the instant case, Plaintiffs have alleged that Google intercepted their communications for the purpose of associating their data with preexisting user profiles. FAC ¶¶ 91, 93, 115, 160–64. The association of Plaintiffs' data with preexisting user profiles is a further use of Plaintiffs' data that satisfies this exception. *See Planned Parenthood Fed'n of Am., Inc., v. Ctr. for Med. Progress*, 21 F. Supp. 3d 808, 828 (N.D. Cal. 2016) (holding that "defendants' subsequent disclosures of the contents of the intercepted conversations for the alleged purpose of further invading the privacy of plaintiffs' staff satisfies" the exception). Indeed, Plaintiffs have adequately alleged that Google's association of their data with preexisting user profiles violated state law, including CDAFA, intrusion upon seclusion, and invasion of privacy. *See* Sections III(C)(3), III(C)(4), *infra*. Accordingly, consent is not a defense to Plaintiffs' Wiretap Act claims. Thus, the Court rejects Google's argument that Plaintiffs consented to the alleged data collection.

2. Google has not shown that the websites consented.

Google next contends that Plaintiffs' Wiretap Act claims should be dismissed because the websites provided implied consent to Google's receipt of the data. Mot. at 11–13. The Wiretap Act provides an exception to liability where "one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(d). Accordingly, Google contends that the websites impliedly consented to Google's alleged data collection by embedding Google's code on their webpages. Mot. at 11–13.

"[A]s 'the party seeking the benefit of the exception,' it is Google's burden to prove consent." *Matera v. Google Inc.*, 2016 WL 5339806, at *17. "Courts have cautioned that implied consent applies only in a narrow set of cases." *In re Google*, 2013 WL 5423918, at *12 (rejecting Google's argument that users had given implied consent, immunizing Google from liability under the Wiretap Act). "The critical question with respect to implied consent is whether the parties whose communications were intercepted had adequate notice of the interception." *Id.* "Moreover, consent is not an all-or-nothing proposition." *Id.* "Rather, '[a] party may consent to the interception of only part of a communication or to the interception of only a subset of its communications.'" *Id.* (quoting *In re Phamatrak*, *Inc.*, 329 F.3d 9, 19 (1st Cir. 2003)). "Thus, 'a reviewing court must inquire into the dimensions of the consent and then ascertain whether the interception exceeded those boundaries.'" *Pharmatrak*, 329 F.3d at 19 (quotation omitted).

Google argues that the websites provided implied consent to Google's interception. Mot at. 11. In making this argument, Google cites two twenty-year-old district court cases regarding DoubleClick (now known as Google Ad Manager), a service which was purchased by websites to gather users' data for advertising purposes. *See Chance v. Avenue A*, 165 F. Supp. 2d 1153, 1160–62 (W.D. Wash. 2001); *In re DoubleClick Privacy Litig.*, 154 F. Supp. 2d 497, 509–11 (S.D.N.Y. 2001). Both district courts concluded that the websites impliedly consented to DoubleClick's interception of their communications with users by installing DoubleClick's code on their websites. *Id*. However, courts have distinguished these cases where "the circumstances permit no reasonable inference that the [entities] did consent." *See, e.g.*, *Pharmatrak*, 329 F.3d at 20.

Google contends that, like the websites in *In re DoubleClick* and *Avenue A*, the websites in the instant case provided implied consent to Google's interception by installing Google's code on their website. Mot at. 11. According to Plaintiffs, the presence of Google's code on the website causes Plaintiffs' browsers to send a duplicate GET request to Google's servers. FAC ¶ 63.

However, the Court concludes that Google has not met its burden to establish consent because, even assuming that Google has established that websites generally consented to the interception of their communications with users, Google does not demonstrate that websites consented to, or even knew about, the interception of their communications with users who were in private browsing mode. Indeed, Google's own resources for "[s]ite or app owners using Google Analytics" state that "[t]he Google privacy policy & principles describes how we treat personal information when you use Google's products and services, including Google Analytics." Schapiro Decl. Exh. 21. Similarly, Google represents to consumers and websites that use Google Ad Manager that Google will adhere to Google's Privacy Policy. FAC ¶ 83.

As the Court explained above, neither Google's Privacy Policy nor any other disclosure to which Google points states that Google engages in the alleged data collection while users are in private browsing mode. *See* Section III(A)(1), *supra*. To the contrary, Google's disclosures present private browsing as a way users can manage their privacy and omits Google from the list of entities to which a user's private browsing activity may be visible. *Id*. Thus, Google has not provided evidence that websites consented to, or even knew about, the interception of the subset of their communications that are with users who were in a private browsing mode. *See Pharmatrak*, 329 F.3d at 19 (explaining that "[a] party may consent to . . . the interception of only a subset of its communications"). Accordingly, Google cannot show implied consent on the part of the websites.[4]

Furthermore, as explained above, consent is not a defense to Plaintiffs' Wiretap Act claim

[4] Plaintiffs allege that, after they filed the instant case, Google launched a "Consent Mode" for Google Analytics and Google Ad Manager, "which would help Websites identify whether a particular user . . . knows and has consented to the use of Google Analytics and other Google services, in 'Beta' or testing mode." FAC ¶¶ 73, 140.

because their communications were allegedly intercepted for the purpose of associating their data with user profiles, which is a criminal or tortious act in violation of the Constitution or laws of the United States or of any State. *See* Section III(A)(1), *supra*. The Court thus rejects Google's consent-based arguments.

B. Statutes of Limitations

Google next argues that Plaintiffs' complaint should be dismissed because each of Plaintiffs' claims exceed the applicable statutes of limitations. Mot. at 23–25. "A claim may be dismissed under Rule 12(b)(6) on the ground that it is barred by the applicable statute of limitations only when 'the running of the statute is apparent on the face of the complaint.'" *Von Saher v. Norton Simon Museum of Art at Pasadena*, 592 F.3d 954, 969 (9th Cir. 2010) (quoting *Huynh v. Chase Manhattan Bank*, 465 F.3d 992, 997 (9th Cir. 2006)). "[A] complaint cannot be dismissed unless it appears beyond doubt that the plaintiff can prove no set of facts that would establish the timeliness of the claim." *Id.* (quoting *Supermail Cargo, Inc. v. United States*, 68 F.3d 1204, 1206 (9th Cir. 1995)).

Each of Plaintiffs' claims has a limitations period of between one and three years. Specifically, the statute of limitations for Plaintiffs' Wiretap Act claim is "two years after the date upon which the claimant first has a reasonable opportunity to discover the violation." 18 U.S.C. § 2520(e). "Under the CIPA, the applicable statute of limitations is one year." *Brodsky v. Apple, Inc.*, 445 F. Supp. 3d 110, 134 (N.D. Cal. 2020). The statute of limitations for Plaintiffs' CDAFA claim is "three years of the date of the act complained of, or the date of the discovery of the damage, whatever is later." Cal. Pen. Code § 502(e)(5). The statute of limitations for Plaintiffs' intrusion upon seclusion and invasion of privacy claims is two years. *See* Cal. Civ. Proc. Code § 335.1 (setting a two year limitations period); *Cain v. State Farm Mut. Auto. Ins. Co.*, 62 Cal. App. 3d 310, 313 (1976) (providing that Section 335.1, formally codified as Section 340, contains the statute of limitations for invasion of privacy claims); *accord Quan v. Smithkline Beecham Corp.*, 149 F. App'x 668, 670 (9th Cir. 2005) (stating that, as of 2003, invasion of privacy is subject to a

two year limitations period).

Google contends that Plaintiffs' claims are barred by the applicable statutes of limitations because Plaintiffs allege that Google has been intercepting their communications since June 1, 2016—over four years before Plaintiffs filed their complaint on June 2, 2020. Mot. at 23. The Court concludes that Plaintiffs' complaint is timely for two reasons. First, each interception is a separate violation, and Plaintiffs allege that Google intercepted their communications between February 28, 2020 and May 31, 2020, just months or weeks before Plaintiffs' complaint was filed. Second, the fraudulent concealment doctrine tolled the statutes of limitations. The Court addresses each issue in turn.

1. Each interception is a separate violation.

First, the Ninth Circuit and California Supreme Court have held that separate, recurring invasions of the same right each trigger their own separate statute of limitations. The Ninth Circuit has held that, for Wiretap Act claims, "each interception is a discrete violation" with its own statute of limitations. *Bliss v. CoreCivic, Inc.*, 978 F.3d 1144, 1148 (9th Cir. 2020). In coming to this conclusion, the Ninth Circuit relied on the Wiretap Act's "multiple references to 'communication' in the singular," which showed that there was "no textual basis for morphing what otherwise would be considered separate violations into a single violation because they flow from a common practice or scheme." *Id*. The Ninth Circuit's reasoning applies to Plaintiffs' other claims, which also refer to "communication" or "act" in the singular. *See* Cal. Penal Code §§ 631(a) (prohibiting the unauthorized interception of "any message, report or communication"); *id*. § 632(a) (prohibiting the interception of a "confidential communication"); Cal. Penal Code § 502(e)(5) (stating that the statute of limitations is three years from "the date of the act complained of, or the date of the discovery of the damage, whichever is later"). Furthermore, the California Supreme Court "ha[s] long settled that separate, recurring invasions of the same right can each trigger their own statute of limitations." *Aryeh v. Canon Business Solutions, Inc.*, 292 P.3d 871, 880 (Cal. 2013).

In the instant case, Plaintiffs allege that Google engaged in interceptions of their communications between February 28, 2020 and May 31, 2020. FAC ¶¶ 168, 173, 178, 183, 188. Plaintiffs filed their complaint on June 2, 2020. ECF No. 1. Because Google's alleged interceptions took place just months or days before Plaintiffs filed their complaint, Plaintiffs' claims are not barred by the statutes of limitations.

2. The statutes of limitations were tolled by the fraudulent concealment doctrine.

"The purpose of the fraudulent concealment doctrine is to prevent a defendant from 'concealing a fraud . . . until such a time as the party committing the fraud could plead the statute of limitations to protect it.'" *In re Animation Workers Antitrust Litig.*, 123 F. Supp. 3d 1175, 1194 (N.D. Cal. 2015) (quoting *Bailey v. Glover*, 88 U.S. (21 Wall) 342, 349 (1874)). "A statute of limitations may be tolled if the defendant fraudulently concealed the existence of a cause of action in such a way that the plaintiff, acting as a reasonable person, did not know of its existence." *Hexcel Corp. v. Ineos Polymers, Inc.*, 681 F.3d 1055, 1060 (9th Cir. 2012). The plaintiff bears the burden of pleading fraudulent concealment. *In re Animation Workers*, 123 F. Supp. 3d at 1194. Fraudulent concealment must be pled with particularity. *Id*. "However, 'it is generally inappropriate to resolve the fact-intensive allegations of fraudulent concealment at the motion to dismiss stage.'" *Id*. (quoting *In re Rubber Chemicals Antitrust Litig.*, 504 F. Supp. 2d 777, 789 (N.D. Cal. 2007)).

"To plead fraudulent concealment, the plaintiff must allege that: (1) the defendant took affirmative acts to mislead the plaintiff; (2) the plaintiff did not have 'actual or constructive knowledge of the facts giving rise to its claim'; and (3) the plaintiff acted diligently in trying to uncover the facts giving rise to its claim." *Id*. (quoting *Hexcel*, 681 F.3d at 1060). The Court addresses each requirement in turn.

First, Plaintiffs have alleged that Google took affirmative acts to mislead Plaintiffs. As explained above, Google's representations regarding private browsing specifically omitted Google from the entities that could see a user's private browsing activity and presented private browsing

as a way that users could maintain their privacy and control what Google collects. *See* Section III(A)(1), *supra*. Accordingly, Google's representations regarding private browsing "obscure[d] Google's intent to engage in such interceptions." *In re Google*, 2013 WL 5423918, at *13. Furthermore, Google's representations were "misleading partial disclosure[s]," which support the application of the fraudulent concealment doctrine. *In re Animation Workers*, 123 F. Supp. 3d at 1203.

Second, Plaintiffs have alleged that they did not have adequate or constructive notice of their claims. "[T]he question of constructive knowledge and inquiry notice generally 'presents a question for the trier of fact.'" *In re Animation Workers*, 123 F. Supp. 3d at 1205. As explained above, Google's representations could have led a reasonable user to conclude that Google was not collecting this data. *See* Section III(A)(1), *supra*. Accordingly, "[a]t this stage, the Court is not persuaded that [Plaintiffs] were on inquiry notice of their claims as a matter of law." *In re Animation Workers*, 123 F. Supp. 3d at 1205.

Finally, Plaintiffs have alleged that they acted diligently in trying to uncover the facts giving rise to their claim. "[C]ourts have 'been hesitant to dismiss an otherwise fraudulently concealed antitrust claim for failure to sufficiently allege due diligence.'" *In re Animation Workers*, 123 F. Supp. 3d at 1205 (quoting *In re Magnesium Oxide Antitrust Litig.*, 2011 WL 5008090, at *24 (D.N.J. Oct. 20, 2011). Google contends that Plaintiffs were not diligent because they failed to "tak[e] Google up on its offer on page 1 of [Google's] Privacy Policy to 'contact us' 'if you have any questions' about Google's practices." Reply at 15 (quoting Schapiro Decl. Exh. 1). That argument "puts the cart before the horse, however, as Plaintiffs were not obligated to investigate their claims until Plaintiffs had reason to suspect the existence of their claims." *In re Animation Workers*, 123 F. Supp. 3d at 1204. Thus, the Court concludes that Plaintiffs have adequately alleged that Plaintiffs' claims were tolled under the fraudulent concealment doctrine.

Because each of Google's interception is a separate violation and because the statutes of limitations were tolled under the fraudulent concealment doctrine, the Court DENIES Google's

motion to dismiss Plaintiffs' claims based on the statutes of limitations.

C. Other Arguments for Dismissal

Finally, Google makes additional arguments that Plaintiffs have failed to state each of their claims. Mot. at 13–23. The Court addresses the following claims in turn: (1) unauthorized interception under the Wiretap Act; (2) CIPA; (3) CDAFA; and (4) intrusion upon seclusion and invasion of privacy.

1. Plaintiffs have stated a claim for unauthorized interception under the Wiretap Act.

The Wiretap Act, as amended by the Electronic Communications Privacy Act ("ECPA"), generally prohibits the interception of "wire, oral, or electronic communications." 18 U.S.C. § 2511(1). Specifically, the Wiretap Act provides a private right of action against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a); *see id.* § 2520 (providing a private right of action for violations of § 2511). The Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4).

Plaintiffs allege that Google violated the Wiretap Act by intercepting internet communications that Plaintiffs were sending and receiving while they were browsing the internet in private browsing mode. FAC ¶¶ 206, 207, 208. Google contends that Plaintiffs have not stated a Wiretap Act claim because its alleged interceptions fall within the Wiretap Act's ordinary course of business exception to liability. Mot. at 13–14. Under that exception, "any telephone or telegraph instrument, equipment or facility, or any component thereof . . . being used by a provider of wire or electronic communication service in the ordinary course of its business" is not a "device," and the use of such an instrument accordingly falls outside of the definition of "intercept." 18 U.S.C. § 2510(5)(a)(ii).

However, Google's argument is unpersuasive for two reasons. First, Google has not shown that its interception facilitates or is incidental to the transmission of the communication at issue.

Second, Plaintiffs have alleged that Google violated its own internal policies. The Court addresses each reason in turn.

First, Google has not shown that its interception facilitates or is incidental to the transmission of the communication at issue. "[T]he ordinary course of business exception is narrow . . . . and offers protection from liability only where an electronic communication service provider's interception facilitates the transmission of *the communication at issue* or is incidental to the transmission of such communication." *In re Google*, 2013 WL 5423918, at *8 (emphasis added); *see also S.D. v. Hytto Ltd.*, 2019 Wl 8333519, at *9 (N.D. Cal. May 15, 2019) (holding that the ordinary course of business exception must be construed "narrowly" and rejecting the exception as to the defendant because the defendant "failed to explain why it would be difficult or impossible to provide its service without the objected-to-interception").

In the instant case, Plaintiffs allege that, whenever a user visits a website, his or her browser sends a GET request to the website's server, which "tells the website what information is being requested and then instructs the website to send the information to the user." FAC ¶ 63. Plaintiffs further allege that Google's code causes the user's browser to send a duplicate GET request from the user's computer to Google's servers, which "enables Google to learn exactly what content the user's browsing software was asking the website to display" and "transmits a . . . header containing the URL information of what the user has been viewing and requesting from websites online." *Id*. ¶¶ 63, 65. Sending a duplicate GET request to Google neither facilitates nor is incidental to the transmission of "the communication at issue," which is the communication that Plaintiffs allege was intercepted — in this case, the communication between the user's computer and the website. *In re Google*, 2013 WL 5423918, at *8.

In an attempt to refute this conclusion, Google contends that the ordinary course of business exception applies because there is a "nexus between the need to engage in the alleged interception and . . . the ability to provide the underlying service or good." *In re Google*, 2013 WL 5423918, at *11. In making this argument, Google contends that the "'underlying service or good'

. . . in this case is [Google's] analytics and ad services," not the communication between the user's computer and the website. Mot. at 13. However, "the communication at issue" is the allegedly intercepted communication, which, in this case, is the communication between the user's computer and the website. *In re Google*, 2013 WL 5423918, at *8. The communication between the user's computer and Google is an unrelated communication. Google's argument to the contrary would vastly expand the ordinary course of business exception by permitting electronic communication services to claim that an interception is in the ordinary course of business when it facilitates another, unrelated communication. This Court has already rejected a similar attempt by Google to expand the ordinary course of business exception beyond its narrow scope. *See In re Google*. 2013 WL 5423918, at *11 (rejecting Google's argument that its interceptions of users' Gmail communications to benefit its advertising business fell within the ordinary course of business exception).

Second, the ordinary course of business exception does not apply because Plaintiffs have alleged that Google violated its own internal policies. As this Court explained in *In re Google*, "Plaintiffs' allegations that Google violated Google's own agreements and internal policies with regard to privacy also preclude application of the ordinary course of business exception." 2013 WL 5423918, at *8. In the instant case, Plaintiffs similarly allege that Google violated its own internal policies with regard to privacy. *See, e.g.*, FAC ¶¶ 42 (Google's statements regarding private browsing), 45 (Privacy Policy), 48 ("Search & browse privately" webpage), 52 (Incognito Splash Screen). Accordingly, the interceptions at issue here do not fall within the ordinary course of business exception, and Plaintiffs have stated a Wiretap Act claim. Thus, the Court DENIES Google's motion to dismiss Plaintiffs' Wiretap Act claim.

2. Plaintiffs have stated a CIPA claim.

Plaintiffs bring claims under Sections 631 and 632 of the CIPA. Section 631 prohibits the unauthorized interception of "any message, report or communication." *See* Cal. Penal Code § 631(a). Section 632 prohibits the interception of any "confidential communication." *Id.* § 632(a).

Google does not argue that the Section 631 claim is subject to dismissal, except based on the consent arguments that the Court has addressed above. *See* Section III(A), *supra*.

Instead, Google contends that Plaintiffs cannot state a Section 632 claim because the communications at issue in this case were not confidential. Mot. at 14–15. A communication is confidential under Section 632 if a party "has an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan v. Flanagan*, 41 P.3d 575, 582 (Cal. 2002). The plaintiff need not show an "additional belief that the information would not be divulged at a later time to third parties." *Mirkarimi v. Nevada Prop. 1 LLC*, 2013 WL 3761530, at *2 (S.D. Cal. July 15, 2013). Rather, the plaintiff only needs to show a reasonable "expectation that the conversation was not being simultaneously disseminated to an unannounced second observer." *Id.*

In arguing that the communications in the instant case were not confidential, Google relies on authority stemming from California appellate courts. "California appeals courts have generally found that Internet-based communications are not 'confidential' within the meaning of [S]ection 632, because such communications can easily be shared by . . . the recipient(s) of the communications." *Campbell v. Facebook, Inc*., 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014). For example, in *People v. Nakai*, the California Court of Appeals held that a defendant's Yahoo instant messages with a decoy, who was posing as a 12-year-old girl, were not confidential. 183 Cal. App. 499, 518–19 (2010). The court concluded that, although the defendant intended for the communication between himself and the recipient to be kept confidential, he could not reasonably expect that the communications would not be recorded. *Id*. at 518. The court came to this conclusion for four reasons. First, Yahoo's policies "indicated that chat dialogues may be shared for the purpose of investigating or preventing illegal activities." *Id.* Second, Yahoo "warn[ed] users that chat dialogues can be 'archive[d], print[ed], and save[d].'" *Id.* Third, "[c]omputers that are connected to the internet are capable of instantaneously sending writings and photographs to thousands of people." *Id.* Finally, the defendant expressed concern that the recipient's mother

would view the messages. *Id*.

Relying on *Nakai*, some cases have held that other Internet messaging services or emails are not confidential under Section 632. For example, in *In re Google*, this Court concluded that email communications were not confidential under Section 632 because "email services are by their very nature recorded on the computer of at least the recipient, who may then easily transmit the communication to anyone else who has access to the internet or print the communications." 2013 WL 5423918 at *23. Similarly, in *Campbell v. Facebook, Inc.*, another court in this district held that Facebook messenger messages were not confidential under Section 632 because they could be shared by the recipients of the communications. 77 F. Supp. 3d at 849. Subsequently, in *Cline v. Reetz-Laiolo*, another court in this district concluded that "emails and other electronic messages" were not confidential communications under Section 632. 329 F. Supp. 3d 1000, 1051–52 (N.D. Cal. 2018).

However, the instant case is distinguishable from this line of authority for two reasons. First, unlike *Nakai*, *In re Google*, or *Campbell*, the instant case does not involve messages going to another person, who could share the communication with others. Rather, the instant case involves a user's own private browsing session. According to Plaintiffs, "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." FAC ¶ 162. For example, users often enable private browsing mode in order to visit especially sensitive websites, which could 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*. Accordingly, Plaintiffs in the instant case could have had a reasonable expectation that their private browsing communications were not being disseminated.

Second, unlike *Nakai*, where Yahoo's policies disclosed that the messages could be shared, Google's policies did not indicate that data would be collected from users in private browsing mode and shared with Google. *See* Section III(A)(1), *supra*. Because the Court concludes that

Nakai and *In re Google* are distinguishable from the instant case, the Court concludes that the communications at issue in this case were confidential.[5] Accordingly, the Court DENIES Google's motion to dismiss Plaintiffs' CIPA claim.

3. Plaintiffs have stated a CDAFA claim.

CDAFA[6] imposes liability on any person who "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network." Cal. Penal Code § 502(c)(2).

Plaintiffs allege that Google violated CDAFA "by knowingly accessing and without permission taking, copying, analyzing, and using Plaintiffs' and Class members' data." FAC ¶ 232. Google contends that this claim should be dismissed because Plaintiffs fail to plausibly allege that Google's Analytics and Ad Manager code circumvented any barrier for Google to receive the data. Mot. at 16.[7]

However, courts have held that plaintiffs can state a CDAFA claim where a software

---

[5] Google also cites *Revitch v. New Moosejaw, LLC*, where another court in this district held that "clicks" on clothing items were not confidential communications. 2019 WL 5485330, at *2 (N.D. Cal. Oct. 23, 2019). However, in coming to that conclusion, the court relied exclusively upon the same line of authority discussed above regarding messages and emails. *Id*. This Court finds that line of authority to be distinguishable from the private browsing sessions involved in the instant case for the reasons explained above.

[6] The CDAFA is also sometimes referred to as the California Computer Crime Law (CCCL). *See Brodsky*, 445 F. Supp. 3d at 131 ("The CCCL is also sometimes referred as the California Comprehensive Computer Data Access and Fraud Act and abbreviated as 'CDAFA.'").

[7] In response to Google's argument, Plaintiffs argue that there is no circumvention requirement. In making this argument, Plaintiffs rely on the Ninth Circuit's decision in *United States v. Christensen*, which concluded that the "term 'access' as defined in the [CDAFA] includes logging into a database with a valid password and subsequently taking, copying, or using the information in the database improperly. Otherwise, the words 'without permission' would be redundant, since by definition hackers lack permission to access a database." 828 F.3d 763, 789 (9th Cir. 2015). However, *Christensen* did not conclude that a barrier need not be circumvented. Rather, *Christensen* held that CDAFA "does not require *unauthorized* access." *Id*. (emphasis in original). Accordingly, *Christensen* still required that a barrier be circumvented—the barrier in that case was a system of password protection.

system "was designed in such a way to render ineffective any barriers that [the plaintiffs] must wish to use to prevent access to their information." *Brodsky v. Apple, Inc.*, 2019 WL 4141936, at *9 (N.D. Cal. Aug. 30, 2019); *see also In re Carrier IQ*, 78 F. Supp. 3d, 1051, 1101 (N.D. Cal. 2015). Indeed, courts have concluded that there is "no reason to distinguish between methods of circumvention built into a software system to render barriers ineffective and those which respond to barriers after they have been imposed." *In re Carrier IQ*, 78 F. Supp. 3d at 1101 (quotation omitted).

For example, another court in this district concluded that the plaintiffs had stated a CDAFA claim about "hidden" software that transmitted data without notice and without providing an opportunity to opt out of its functionality. *See In re Carrier IQ*, 78 F. Supp. 3d, 1051, 1101 (N.D. Cal. 2015). The court concluded that this software "would effectively render any 'technical or code based' barrier implemented by the Plaintiffs ineffective." *Id*. Accordingly, the court concluded that the plaintiffs had stated a CDAFA claim. *Id*.

Similarly, Plaintiffs have adequately alleged a CDAFA claim in the instant case because Plaintiffs allege that Google's Analytics and Ad Manager core would render ineffective any barrier that Plaintiffs implemented. Specifically, Plaintiffs allege that Google's hidden code, like the software at issue in *In re Carrier Q*, transmitted data without notice while they were in private browsing mode. FAC ¶ 63 (describing how Google's hidden code directs the user's browser to send a duplicate request to Google). Furthermore, Plaintiffs allege that there was no opportunity to opt out of Google's hidden code, as was the case in *In re Carrier Q*. Thus, like the software at issue in *In re Carrier Q*, Google's hidden code would render ineffective any barrier Plaintiffs wished to use to prevent the transmission of their data. Accordingly, Plaintiffs have adequately stated a CDAFA claim, and the Court DENIES Google's motion to dismiss this claim.

4. Plaintiffs have stated claims for intrusion upon seclusion and invasion of privacy.

"To state a claim for intrusion upon seclusion under California common law, a plaintiff must plead that (1) a defendant 'intentionally intrude[d] into a place, conversation, or matter as to

which the plaintiff has a reasonable expectation of privacy[,]' and (2) the intrusion 'occur[red] in a manner highly offensive to a reasonable person." *Facebook Tracking*, 956 F.3d at 601 (quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (2009)). "A claim for invasion of privacy under the California Constitution involves similar elements. Plaintiffs must show that (1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is 'so serious . . . as to constitute an egregious breach of the social norms' such that the breach is 'highly offensive.'" *Id*. (quoting *Hernandez*, 47 Cal. 4th at 287). "Because of the similarity of the tests, courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *Id*. The Court addresses each element in turn.

a. Plaintiffs have adequately alleged that they had a reasonable expectation of privacy.

To meet the first element, the plaintiff must have had an "objectively reasonable expectation of seclusion or solitude in the place, conversation, or data source." *Shulman v. Group W. Prods., Inc.*, 18 Cal. 4th 200, 231 (1998). "[T]he relevant question here is whether a user would reasonably expect that [Google] would have access to the . . . data." *Facebook Tracking*, 956 F.3d at 602.

In *Facebook Tracking*, the Ninth Circuit considered whether the plaintiffs, who were Facebook users, had adequately pleaded that they had a reasonable expectation of privacy. *Id*. at 602. Like the instant case, *Facebook Tracking* concerned GET requests that were sent from Facebook users' browsers to Facebook after they had logged out of Facebook. *Id*. at 601. Like Google, Facebook allegedly received copies of GET requests that users sent to third-party websites because Facebook's embedded code caused the users' browses to generate copies of the GET requests and transmit them to Facebook. *Compare id*. at 607 *with* FAC ¶ 63.

The Ninth Circuit concluded that the plaintiffs had adequately pleaded that they had a reasonable expectation of privacy based on: (1) the amount of the data collected, the sensitivity of the data collected, and the nature of the data collection, and (2) Facebook's representations to

users. *Facebook Tracking*, 956 F.3d at 602. The Court discusses each issue in turn.

The Ninth Circuit assessed the amount of the data collected, the sensitivity of the data collected, and the nature of the data collection. *Id*. at 603. The Ninth Circuit concluded that "the amount of data allegedly collected was significant"; Plaintiffs alleged that "Facebook obtained a comprehensive browsing history of an individual" and "then correlated that history with the time of day and other user actions on the websites visited," resulting in "an enormous amount of individualized data." *Id.* Additionally, the Ninth Circuit emphasized that some of the alleged data collected was sensitive, such as information about a user's visits to sensitive websites. *Id*. Finally, the Ninth Circuit found it significant "[t]hat this amount of information can be easily collected without user knowledge." *Id*.

In addition, the Ninth Circuit examined Facebook's representations to users. *Id*. According to the Ninth Circuit, "Plaintiffs . . . plausibly alleged that an individual reading Facebook's promise to 'make important privacy disclosures' could have reasonably concluded that the basics of Facebook's tracking—when, why, and how it tracks user information—would be provided." *Id*. However, "Facebook's privacy disclosures at the time allegedly failed to acknowledge its tracking of logged-out users, suggesting that users' information would not be tracked." *Id.* Accordingly, "Plaintiffs . . . plausibly alleged that, upon reading Facebook's statements in the applicable Data Use Policy, a user might assume that only logged-in user data would be collected." *Id*.

Other cases have come to similar conclusions. For example, in *Google Cookie*, the Third Circuit considered whether the plaintiffs had stated intrusion upon seclusion and invasion of privacy claims under California law. 806 F.3d 125, 149 (3d. Cir. 2015). That case concerned Google's placement of cookies on the browsers of users who had enabled cookie blockers. *Id*. at 132. The Third Circuit concluded that the plaintiffs had a reasonable expectation of privacy based on "how Google accomplished its tracking," which involved "overriding the plaintiffs' cookie blockers, while concurrently announcing in its Privacy Policy that internet users could 'reset your browser to refuse all cookies.'" *Id*. at 151.

Similarly, in *In re Nickelodeon Consumer Privacy Litigation*, the Third Circuit considered whether the plaintiffs had stated a claim for intrusion upon seclusion under New Jersey law. 27 F.3d 262, 293–94 (3d. Cir. 2016). The plaintiffs alleged that Nickelodeon had placed cookies on users' browsers despite promising that it would not collect information from the users of its website. *Id*. The Third Circuit held that users had a reasonable expectation of privacy when Nickelodeon promised that it would not collect information from users of its website, but then did. *Id*.

In the instant case, Court concludes that Plaintiffs have adequately alleged that they had a reasonable expectation of privacy in the data allegedly collected for two reasons. First, the amount of data collected, the sensitivity of the data collected, and the nature of the data collection demonstrate that Plaintiffs have a reasonable expectation of privacy. Second, based on Google's representations regarding private browsing, Plaintiffs could have reasonably assumed that Google would not receive their data while they were in private browsing mode. The Court discusses each reason in turn.

First, Plaintiffs have adequately alleged that they had a reasonable expectation of privacy based on the amount of data collected, the sensitivity of the data collected, and the nature of the data collection. Indeed, the instant case involves the same data and the same process by which the data was collected as *Facebook Tracking*. *Compare id*. at 607 (describing how Facebook's code directs the user's browser to copy the referrer header and sends a duplicate request to Facebook) *with* FAC ¶ 63 (describing how Google's code directs the user's browser to send a duplicate request to Google). Even Google acknowledges the similarities between the two cases. *See* Tr. of Feb. 25, 2021 Hearing at 9:16–21, ECF No. 104 (The Court: "Let me ask Google's counsel, do you agree that the data [at] issue in this case is the same as the data at issue in *Facebook Tracking* like Plaintiffs' counsel just said?" Counsel: "Yes, much of the - - I would say yes, most of the data, probably all of it, is the same if we take [Plaintiffs] at their word for what we've just heard from [Plaintiff's counsel].").

The amount of data collected, the sensitivity of the data collected, and the nature of the data collection demonstrate that Plaintiffs had a reasonable expectation of privacy. Like in *Facebook Tracking*, Plaintiffs allege that the amount of data collected was vast. *See* FAC ¶ 8 (alleging that "[m]ore than 70% of all online publishers (websites) use one or more of [the] Google services" that collect data); *id*. ¶ 93 (alleging that "Google has gained a complete, cradle-to-grave profile of users"). Moreover, Plaintiffs' allegations regarding the sensitivity of the data collected are arguably even stronger in the instant case than in *Facebook Tracking*. Indeed, the instant case concerns data collected by users in private browsing mode, which users often enable in order to visit especially sensitive websites. *Id*. ¶ 162 ("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. For example, 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)."). Finally, like in *Facebook Tracking*, Plaintiffs allege that a vast amount of data was collected secretly, without any notice to users. *Id*. ¶¶ 63 (describing how "Google's software scripts on the website surreptitiously direct the user's browser to send a secret, separate message to Google's servers"); 87 (describing how "Google's secret Javascript code" causes duplicate GET requests to be sent).

Second, like the plaintiffs in *Facebook Tracking*, Plaintiffs in the instant case could have reasonably assumed that Google would not receive their data while they were in private browsing mode based on Google's representations. Since May 25, 2018, Google's Privacy Policy itself has presented private browsing as a way that users can manage their privacy: "You can use our services in a variety of ways to manage your privacy. For example, . . . [y]ou can . . . choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used." Schapiro Decl. Exh. 8. Similarly, the Incognito Splash Screen states: "You've gone incognito[.]

Now you can browse privately, and other people who use this device won't see your activity[.]" FAC ¶ 52. Furthermore, on the Incognito Splash Screen and in other webpages, Google discloses that a user's activity in private browsing might be visible to certain entities, but Google does not identify itself as an entity to which a user's activity might be visible. Schapiro Decl. Exh. 19; FAC ¶ 52.

Despite the similarities between *Facebook Tracking* and the instant case, Google attempts to distinguish *Facebook Tracking* on two grounds. First, Google contends that Plaintiffs in the instant case consented to the alleged data collection. Second, Google contends that Plaintiffs have not adequately alleged that Google is associating data with personal profiles. Both arguments are unpersuasive.

First, Google contends that, unlike the plaintiffs in *Facebook Tracking*, Plaintiffs in the instant case consented to the alleged data collection. However, as the Court explained above, Plaintiffs did not consent to the alleged data collection. *See* Section III(A)(1), *supra*. Rather than disclosing the alleged data collection to users, Google made representations that could suggest to a reasonable user that the data would not be shared with Google while the user was in private browsing mode. *Id*.

Second, Google argues that, unlike in *Facebook Tracking*, Plaintiffs here have not adequately alleged that Google is associating data with personal profiles. However, like the Plaintiffs in *Facebook Tracking*, Plaintiffs have alleged that Google "obtained a comprehensive browsing history of an individual, no matter how sensitive the websites visited." 956 F.3d at 603. Indeed, Plaintiffs' complaint includes a section titled "Google Creates a User Profile on Each Individual." *See* FAC ¶ 92. That section alleges that "Google has gained a complete, cradle-to-grave profile of users." *Id*. ¶ 93. As to data gathered from users in private browsing mode, Plaintiffs allege that "[i]n many cases, Google is able to associate the data collected from users in 'private browsing mode' with specific and unique user profiles through Google Analytics User-ID. Google does this by making use of a combination of the unique identifier of the user it collects

from Websites, and Google Cookies that it collects across the internet on the same user." *Id*. Plaintiffs also allege that Google supplements its profiles with the X-Client Data Header, fingerprinting techniques, system data, and geolocation data. *Id*. ¶¶ 94–112. Accordingly, Google's arguments are unpersuasive. Thus, Plaintiffs have alleged that they have a reasonable expectation of privacy in their data.

b. Plaintiffs have adequately alleged that the alleged intrusion was highly offensive.

"Determining whether a defendant's actions were 'highly offensive to a reasonable person' requires a holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive." *Facebook Tracking*, 956 F.3d at 606 (quoting *Hernandez*, 47 Cal. 4th at 287). "While analysis of a reasonable expectation of privacy primarily focuses on the nature of the intrusion, the highly offensive analysis focuses on the degree to which the intrusion is unacceptable as a matter of public policy." *Id*. (citing *Hernandez*, 47 Cal. 4th at 287).

In *Facebook Tracking*, the Ninth Circuit held that "[t]he ultimate question of whether Facebook's tracking and collection practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage." *Id*. Specifically, the Ninth Circuit concluded that "Plaintiffs' allegations of surreptitious data collection when individuals were not using Facebook are sufficient to survive a dismissal motion on the issue" of whether the alleged intrusion was highly offensive. *Id*. In coming to this conclusion, the Ninth Circuit emphasized that "Plaintiffs have alleged that internal Facebook communications reveal that the company's own officials recognized these practices as a problematic privacy issue." *Id*.

As explained above, Plaintiffs in this case allege that Google was surreptitiously collecting the same type of data through the same process that was at issue in *Facebook Tracking*. *See* Section III(C)(4)(a), *supra*. Furthermore, Plaintiffs in the instant case have an even stronger argument that Google's intrusion was highly offensive because, at the time Google collected the

data, they were using private browsing mode, which is often used to prevent others from learning the user's most private and personal interests. FAC ¶ 162 ("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. For example, 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).").

Moreover, as explained above, Google's representations regarding private browsing mode could have led users to assume that Google would not view their activity while in private browsing mode. *See* Section III(A)(1), *supra*. Furthermore, like the plaintiffs in *Facebook Tracking*, Plaintiffs also allege that internal Google communications show that the company's employees recognized that its privacy disclosures were problematic. FAC ¶ 36 (alleging that "Google's employees made numerous admissions in internal communications, recognizing that Google's privacy disclosures are a 'mess' with regards to obtaining 'consent' for its data collection practices and other issues relevant in this lawsuit").

Google argues that its conduct is not "highly offensive" because its interceptions "served a legitimate commercial purpose." Mot. at 22. However, whether an intrusion is highly offensive requires a holistic consideration of a multitude of factors, only one of which is the "countervailing interests . . . [that] render the intrusion inoffensive," such as the intrusion's commercial purpose. *See Facebook Tracking*, 956 F.3d at 606 (quoting *Hernandez*, 47 Cal. 4th at 287). Recognizing this, the Ninth and Third Circuits have concluded that plaintiffs had sufficiently alleged that similar intrusions to the one at issue in the instant case are highly offensive. *See id.* (holding that the plaintiffs had sufficiently alleged that Facebook's collection of duplicate copies of GET requests from users who were signed out was highly offensive); *Google Cookie*, 806 F.3d at 150 (concluding that the plaintiffs had sufficiently alleged that Google's practice of circumventing cookie blockers was highly offensive). Indeed, in *Google Cookie*, the Third Circuit rejected a

similar argument by Google. 806 F.3d at 150. Although Google argued that "tracking cookies are routine," the court concluded that "[b]ased on the pled facts, a reasonable factfinder could indeed deem Google's conduct 'highly offensive.'" *Id.* at 150–51. The Court comes to the same conclusion in the instant case.

Thus, Plaintiffs have alleged sufficient facts to survive a motion to dismiss on the issue of whether the intrusion was highly offensive. Accordingly, Plaintiffs have stated intrusion upon seclusion and invasion of privacy claims. Therefore, the Court DENIES Google's motion to dismiss these claims.

IV. CONCLUSION

For the foregoing reasons, the Court DENIES Google's motion to dismiss.

IT IS SO ORDERED.

Dated: March 12, 2021

Lucy H. Koh

LUCY H. KOH
United States District Judge