United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

RODRIGUEZ, et al., Plaintiffs, v. GOOGLE LLC, Defendant.	Case No. 20-cv-04688-RS **ORDER GRANTING IN PART & DENYING IN PART MOTION TO DISMISS**

I. INTRODUCTION

Defendant Google LLC ("Google") is in the business of collecting internet users' data. Of the many ways it plies this trade, one entails providing services to the developers of third-party internet applications. Anibal Rodriguez, JulieAnna Muniz, and seven other named plaintiffs (together, "plaintiffs") are internet users—and, more particularly, users of third-party apps to which Google provides services. Seeking putative classwide relief under the federal Wiretap Act and California law, they claim Google's relationship with these apps results in illegal data collection. This argument runs down two independent narrative tracks: in plaintiffs' view, Google's liability flows from both (i) Google technology that, when functioning as advertised in a given app, contravenes the company's user-facing privacy representations, and (ii) "secret" software, hidden within that technology, that trawls for data on Google's behalf unbeknownst to users and app developers alike. Google denies the "secret" software's existence, and now moves to dismiss on the theory that its challenged data practices enjoy the consent of all involved. For the reasons set forth herein, the motion is granted in part, and denied in part.

United States District Court
Northern District of California

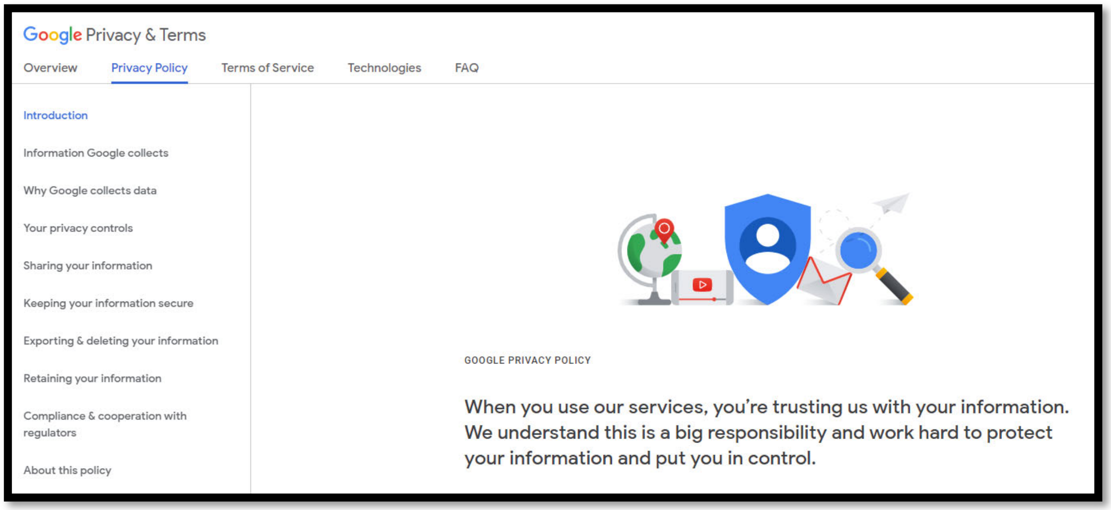
II. BACKGROUND[1]

A. Google's User Privacy Framework

Google, no stranger to privacy disputes, currently maintains a complex user-facing[2] privacy apparatus. Two aspects of this framework pertain here.

1. Privacy and Terms

Google's Privacy and Terms website serves as a hub of the firm's consumer privacy representations. Through its layout, this site invites toggling between five different privacy-related sections.



GOOGLE PRIVACY POLICY

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

First Amended Complaint ("FAC") ¶ 106 n.41, Dkt. 60 at 34 (linking to this page).

In the "Technologies" section, under the sub-heading "How Google uses information from sites or apps that use our services," Google states:

> Many websites and apps use Google services to improve their content and keep it free. When they integrate our services, these sites and apps share information with Google.

[1] This order draws on various non-pleadings materials. By affirmatively engaging with these materials, both in briefing and at oral argument, the parties have waived any objections as to the propriety of their being judicially noticed. *See* Tr., Dkt. 98 at 51-52.

[2] As distinct from enterprise-facing.

> . . .
>
> Sometimes, when processing information shared with us by sites and apps, those sites and apps will ask for your consent before allowing Google to process your information . . . . When that happens, we will respect the purposes described in the consent you give the site or app, rather than the legal grounds described in the Google Privacy Policy. If you want to change or withdraw your consent, you should visit the site or app in question to do so.

Elsewhere, in the "Privacy Policy" section, Google states:

> Our services include:
>
> - Google apps, sites, and devices, like Search, YouTube, and Google Home
> - Platforms like the Chrome browser and Android operating system
> - Products that are integrated into third-party apps and sites, like ads and embedded Google Maps

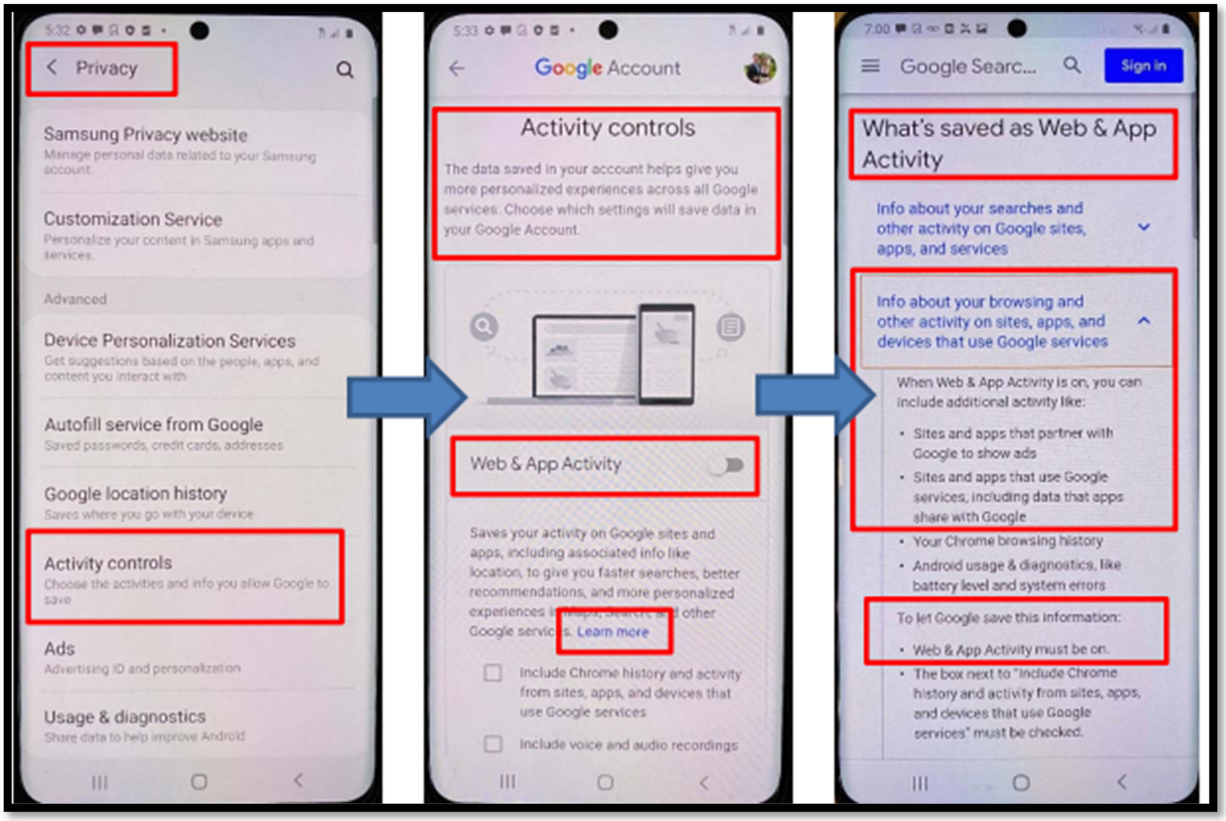
Further down the "Privacy Policy" page, under the sub-heading "Ways to review and update your information," Google presents a hyperlink to the "My Activity" portal, which "allows you to review and control data that's created when you uses Google services[.]" By clicking the "My Activity" hyperlink and a series of additional hyperlinks, a Privacy & Terms website visitor is directed to the "Web & App Activity" ("WAA") feature.

2. Web & App Activity

Accessible by both the above-described process and the settings menu of certain smart devices, the WAA feature purports to give consumers control over a defined subset of Google's data-gathering efforts. Specifically, across the suite of landing pages presenting and explaining the feature (the "WAA Materials"), Google represents that turning WAA on or off dictates "[t]he data saved in" an individual's "Google Account"; that such data includes "info about [the individual's] searches and other activity on Google sites, apps, and services," as well as "info about [the individual's] . . . activity on sites, apps, and devices that use Google services"; and that "[t]o let Google save this information . . . Web & App Activity must be on."

//

//



5:32

< Privacy

Samsung Privacy website
Manage personal data related to your Samsung account.

Customization Service
Personalize your content in Samsung apps and services.

Advanced

Device Personalization Services
Get suggestions based on the people, apps, and content you interact with

Autofill service from Google
Saved passwords, credit cards, addresses

Google location history
Saves where you go with your device

Activity controls
Choose the activities and info you allow Google to save

Ads
Advertising ID and personalization

Usage & diagnostics
Share data to help improve Android

5:33

Google Account

Activity controls

The data saved in your account helps give you more personalized experiences across all Google services. Choose which settings will save data in your Google Account.

Web & App Activity

Saves your activity on Google sites and apps, including associated info like location, to give you faster searches, better recommendations, and more personalized experiences in Maps, Search, and other Google services. Learn more

□ Include Chrome history and activity from sites, apps, and devices that use Google services

□ Include voice and audio recordings

7:00

Google Searc... Sign in

What's saved as Web & App Activity

Info about your searches and other activity on Google sites, apps, and services

Info about your browsing and other activity on sites, apps, and devices that use Google services

When Web & App Activity is on, you can include additional activity like:

- Sites and apps that partner with Google to show ads
- Sites and apps that use Google services, including data that apps share with Google
- Your Chrome browsing history
- Android usage & diagnostics, like battery level and system errors

To let Google save this information:

- Web & App Activity must be on.
- The box next to "Include Chrome history and activity from sites, apps, and devices that use Google services" must be checked.

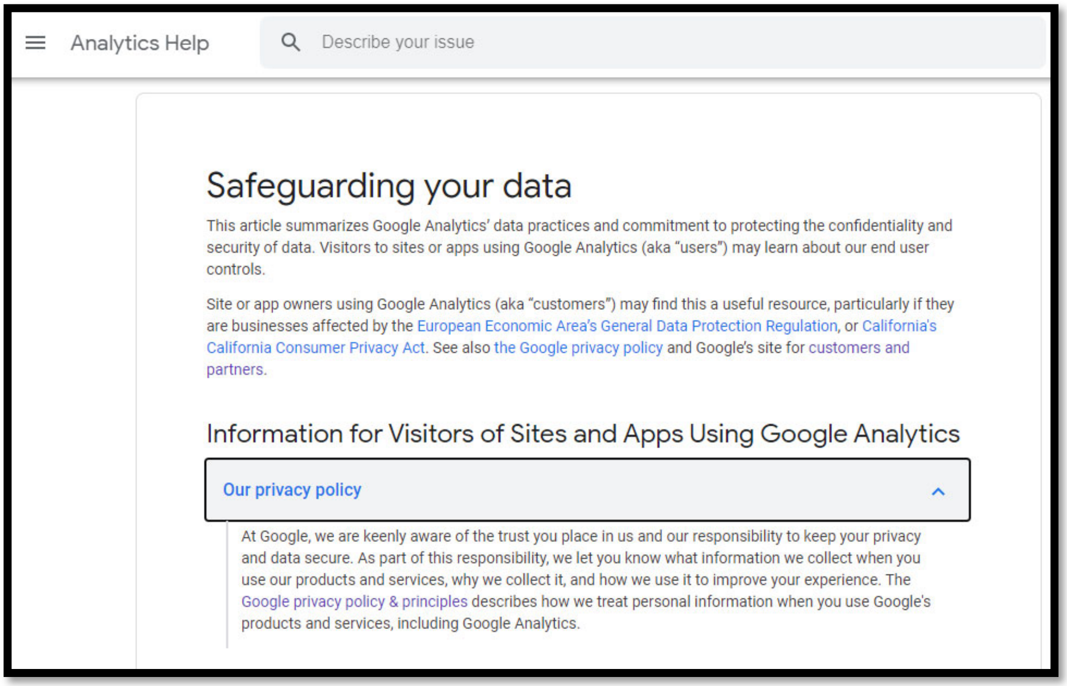
FAC ¶ 71, Dkt. 60 at 23 (displaying these screenshots). Unlike the Privacy and Terms page, the WAA Materials do not define or list "Google services." Neither the WAA Materials nor the Privacy and Terms hub defines "Google Account."

B. Google Analytics for Firebase

Separately, on the enterprise-facing side of its operations, Google offers a free software development kit, called Firebase SDK ("Firebase"), to third-party app developers. Best understood as a digital "toolkit," Firebase comprises eighteen distinct "tools," some of which an app creator must use to build and maintain an app, and others of which a creator may use. Google Analytics for Firebase ("GA for Firebase") falls into the second group: should an app developer elect to use it, GA for Firebase will automatically send various interactions between the app and its users (including the users' URL requests, in-app browsing history, and in-app search queries) to Google, which will then present a clean, optimization-minded analysis of that data to the developer.

In connection with a developer's decision to use GA for Firebase, Google provides the developer with a suite of agreements, policies, and resources (the "GA for Firebase Materials").

These documents are noteworthy for three reasons. First, the GA for Firebase Materials require that, prior to enabling GA for Firebase, a developer affirmatively consent to the product's "incorporat[ion] in [the] App for the purpose of collecting Consumer Data." Second, they oblige the developer to "disclose the use of the [GA for Firebase] Service, and how it collects and processes data," to app users, and to "use commercially reasonable efforts to ensure" each user "consents to" that practice. Finally, the GA for Firebase Materials furnish assorted disclosures that "app owners . . . may find . . . useful," including "Information for Visitors of Sites and Apps Using Google Analytics."[3] One such piece of information, labelled "Our privacy policy," advises that "[t]he Google privacy policy and principles describes how we treat personal information when you use Google's products and services, including Google Analytics."



Safeguarding your data

This article summarizes Google Analytics' data practices and commitment to protecting the confidentiality and security of data. Visitors to sites or apps using Google Analytics (aka "users") may learn about our end user controls.

Site or app owners using Google Analytics (aka "customers") may find this a useful resource, particularly if they are businesses affected by the European Economic Area's General Data Protection Regulation, or California's California Consumer Privacy Act. See also the Google privacy policy and Google's site for customers and partners.

Information for Visitors of Sites and Apps Using Google Analytics

Our privacy policy

At Google, we are keenly aware of the trust you place in us and our responsibility to keep your privacy and data secure. As part of this responsibility, we let you know what information we collect when you use our products and services, why we collect it, and how we use it to improve your experience. The Google privacy policy & principles describes how we treat personal information when you use Google's products and services, including Google Analytics.

[3] These disclosures are catalogued in a "Help Center," which the FAC characterizes as the "[h]elp page intended for use by app developers who use Firebase SDK." *See* FAC ¶ 105, Dkt. 60 at 33. While strictly true, this characterization belies the fact that the "Help Center" is also "intended for use" by *anyone* (not just developers) who is curious about Google Analytics generally (not just GA for Firebase). Users, for instance, may access the "Help Center" from the Privacy and Terms website. Because, however, Google has not challenged the notion that the representations made in this "Help Center" are, for purposes of testing developers' contractual expectations, made "to" developers using GA for Firebase, this analysis places those representations under the "GA for Firebase Materials" rubric.

United States District Court
Northern District of California

FAC ¶ 105, Dkt. 60 at 34 (displaying this screenshot). By clicking on the hyperlinked phrase "Google privacy policy & principles," one arrives at the Privacy and Terms website.

C. Alleged Misconduct

Plaintiffs object to Google's collection of their interactions with apps built atop Firebase.[4] As previously mentioned, this objection takes two forms. First, concerning Firebase's disclosed functionality, plaintiffs allege Google's capture and analysis of data via GA for Firebase, on behalf of app developers who knowingly utilize that service, violates the WAA Materials' representations to individuals who have disabled the WAA feature. Under this theory of liability, GA for Firebase—when running as marketed—allows Google to collect information about an individual's "activity on . . . apps . . . that use Google services," notwithstanding the WAA Materials' statement that "[t]o let Google save this information . . . Web & App Activity *must* be on." (Emphasis added). Second, concerning Firebase's *undisclosed* functionality, plaintiffs claim Google hides "secret scripts" (*i.e.*, secret lines of code) throughout the Firebase toolkit, which in turn "collect data from user communications with [Firebase] apps and send that data to Google servers[.]" Under this separate, more sinister theory of liability, Google's offense rises above upsetting privacy expectations set by the WAA Materials, to the level of outright fraud.

Distinct from GA for Firebase in that they are known only to Google, these "secret scripts" nevertheless are, per the FAC, strikingly similar in practice to GA for Firebase. Indeed, elaborating on what types of data the "secret scripts" ostensibly collect, the FAC links to a webpage describing the data collection process for GA for Firebase. In this fashion, plaintiffs' "secret scripts" narrative seems to distill to Google's alleged practice of embedding a "shadow" version of GA for Firebase, for its own exclusive benefit, within other of the Firebase toolkit's

[4] From the roughly 1.5 million apps using Firebase, plaintiffs identify nine in the FAC, including the mobile apps of the New York Times, The Economist, and NPR. All nine of these identified apps are "free" in the sense that no fee is required for their download and basic use. Even so, the FAC contains a lone assertion that "[p]laintiffs and [c]lass members . . . paid for certain apps whereby Google received money from [p]laintiffs and [c]lass members[.]" FAC ¶ 313, Dkt. 60 at 78.

eighteen constituent tools. Though plaintiffs' briefing suggests these clandestine dragnets operate regardless of whether GA for Firebase is running in the underlying app, the FAC omits that assertion.

III. LEGAL STANDARD

A complaint must contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). A motion to dismiss for failure to meet this standard may be based either on the "lack of a cognizable legal theory" or on "the absence of sufficient facts alleged under a cognizable legal theory." *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1990). Additionally, when a party lodges "allegations of fraud or mistake," that party "must state with particularity the circumstances constituting fraud and mistake." Fed. R. Civ. P. 9(b). In this setting, a plaintiff must plead "the who, what, when, where, and how that would suggest fraud." *Cooper v. Pickett*, 137 F.3d 616, 627 (9th Cir. 1997) (internal quotation marks omitted).

IV. DISCUSSION

Plaintiffs advance six claims for relief, under (i) section 2511(1)(a) of the Wiretap Act, (ii) sections 631 and 632 of the California Invasion of Privacy Act ("CIPA"), (iii) the California Computer Data Access and Fraud Act ("CDAFA"), (iv) California's common law right against intrusion upon seclusion, (v) California's constitutional proscription of invasion of privacy, and (vi) California's Unfair Competition Law ("UCL"). While claims (iii)-(v), along with the section 631 component of claim (ii), withstand Google's 12(b)(6) attack, the remainder do not. This conclusion rests in large part on three threshold determinations. As a pleading matter, plaintiffs did not consent to Google collecting their data, through GA for Firebase, with WAA turned "off"; developers did consent to such data collection; and Google has not deployed any "secret scripts."

A. User Consent

Plaintiffs do not deny, for each app at issue, reading and agreeing to a developer-generated disclosure—made at Google's behest—outlining the "use of the [GA for Firebase] Service . . . [to] collect[] and process[] data." Instead, combining (i) the WAA Materials' statement that WAA "must be on" in order "[t]o let Google save . . . information" concerning activity on apps "that use Google services," and (ii) the Privacy Policy's definition of "services" as including "[p]roducts that are integrated into third-party apps, like ads and embedded Google Maps," they claim to have interpreted the WAA feature as superseding those app-specific disclosures. Google counters that this interpretation is too unreasonable to serve as a plausible basis for relief. For three reasons, Google's argument misses the mark.

First, plaintiffs' construction of the phrase "Google services" is, despite Google's protestations, hardly far-fetched. Because the WAA Materials use the phrase without defining it, plaintiffs resort to the definition offered by the Privacy Policy. On its face, that definition permits the inference that GA for Firebase is a "Google service"—that is, a "[p]roduct[] that [is] integrated into third party apps[.]" Rather than spilling ink to suggest otherwise, Google latches onto the definition's subordinate clause: "like ads and embedded Google Maps[.]" In an apparent application of the *esjudem generis* rule, Google maintains this clause narrows its antecedent to those services that are "aimed at users," thereby excluding GA for Firebase. *See* Reply, Dkt. 82 at 13. Put bluntly, this position assigns "ads and embedded Google Maps" more weight than they can bear. Even if users were, as a matter of law, precluded from bringing claims in tension with select interpretative canons, Google does not explain how "ads and embedded Google Maps," listed together, necessarily connote user-facing services. To the contrary, Google's advertising products would seem to be quintessentially *enterprise*-facing: unlike Maps, Search, and YouTube (from which users derive immediate value), advertisements, like GA for Firebase, go chiefly to developers' behind-the-scenes interests and operations. Plaintiffs' idea of what "Google services" means is therefore entirely plausible, and not made less so by Google's artful word-parsing.

Second, the WAA Materials' statement that turning WAA on or off governs whether data is "saved in" a user's "Google Account" does not clearly exclude GA for Firebase from the WAA feature's operative scope. This finding follows another: the concept of a "Google Account" is, at best, nebulous. Asked, for instance, to define it at the hearing for this motion, Google's counsel noted "there's an account creation process . . . involv[ing] assigning an email address and making certain disclosures"; acknowledged the nominal distinction between data stored by Google "in" a Google Account, when WAA is turned "on," and data stored by Google elsewhere; and carried on with his argument. *See* Tr., Dkt. 98 at 28-31. Working off this response and other scattered descriptions of discrete Google Account *features*—as opposed to, say, a succinct, plain English explanation of what exactly a Google Account *is*—one might hazard to construe the Google Account offering as (i) a Google service available to any individual with an email address, that (ii) monitors the individual's activity across all of Google's user-facing services (Gmail, Chrome, Google Search, Google Maps, etc.), across all digital devices (laptop, smart-phone, tablet, etc.), and (iii) "personalizes" the individual's experiences of those services accordingly. Yet plaintiffs' failure to grasp as much—in the absence of any guidance from the WAA Materials, Privacy and Terms portal, or any other Google resource identified in this litigation—simply cannot count against them. The average internet user is not a full-stack engineer; he or she should not be treated as one when Google explains which digital data goes into which digital buckets, and where the corresponding spigots might be found. That plaintiffs did not first perceive the precise contours of a Google Account, before arriving at their averred understanding of the WAA feature, does not doom their claims.

Finally, and in a related vein, Google's gripe that plaintiffs attempt to pass WAA off as "a single valve that can control the entire flow of data on the Internet" falls on less-than-sympathetic ears. *See* Reply, Dkt. 82 at 14. As the present controversy throws into sharp relief, navigating Google's user-facing privacy representations is a singularly fragmented affair.[5] On the one hand,

[5] Consider this: per Google, a *correct* interpretation of the WAA feature's functionality synthesizes (i) one landing page's statement of what happens when WAA is "on," (ii) the preceding landing page's mention of "your Google Account," (iii) working knowledge of what a Google Account is (presumably drawn from a series of separate webpages), (iv) a strained reading of the Privacy Policy's definition of "Google Services" (as provided in one of the five sections of Google's Privacy and Terms hub), and (v) familiarity with Google's custom of "respect[ing] the purposes described in the consent [users] give to [third-party] app[s] or site[s], rather than the legal grounds described in the Google Privacy Policy" (as set out in one of the sub-headings of a different section of the Privacy and Terms hub). Similarly, on point (v), it bears noting that the WAA Materials' strongest statement ("[t]o let Google save this information . . . Web & App Activity *must* be on") is at least three hyperlinks removed from the Privacy Policy. (Emphasis added). Google does not attempt to explain, via the incorporation-by-reference doctrine or some

this unfortunate reality is to be expected—after all, complex business makes for complex fine print. On the other, it does not follow that Google evades blame for the accompanying fallout. Where, as here, a company's public-facing statements are legitimately confusing, it is not the public's fault for being confused. The insinuation of Google's "single valve" critique—namely, that plaintiffs' estimation of the WAA feature is so naïve (or disingenuous) as to be legally deficient—is thus misguided. Plaintiffs offer a cogent account of why they saw WAA as capable of turning off GA for Firebase's collection of their third-party app data; and Google, for all its efforts, does not succeed in casting this account as implausible. On the pleadings, plaintiffs did not consent to the practice they now challenge.

B. Developer Consent

Fortunately for Google, the developer consent issue breaks in the opposite direction. Plaintiffs concede developers knowingly agree to GA for Firebase "collecting Consumer Data," and do not argue developers somehow misapprehend the product's general function or purpose. Still, foregrounding the GA for Firebase Materials' purported incorporation of Google's entire privacy framework,[6] they insist developers contemplate GA for Firebase collecting user data only insofar as that collection comports with each user's individual privacy expectations. Under this "consent-upon-consent" rationale, an app creator's agreement to use GA for Firebase ends precisely where a user's plausible interpretation of a conflicting privacy setting (in this case, WAA) begins. Plaintiffs cite no authority adopting this reasoning—and, more tellingly, do not grapple with its plainly untenable real-world implications.

Suppose, as plaintiffs do, that developers consent to a specific Google service on the understanding that it will only be provided consistent with *every* defensible reading of *every*

other principle of law, how that statement is a "legal ground[] described *in* the Google Privacy Policy." (Emphasis added).

[6] Recall that, in the GA for Firebase Materials' statement that "[t]he Google privacy policy and principles describes how we treat personal information when you use Google's products and services, including Google Analytics," the phrase "Google privacy policy and principles" hyperlinks to the Privacy and Terms portal.

representation Google makes to *each* of its counterparties.[7] How would Google—or any firm operating in a multi-counterparty marketplace—carry on its business? Take the example of an organic snack start-up: it maintains an email marketing list, which it entices customers to join by promising "never to sell your data." Before the company can secure a booth for handing out samples at Local Grocer, Local Grocer requires it to send an email to that list, imploring people to "come see us this weekend at Local Grocer!" The email upsets certain of the list's members, who sincerely feel their email addresses were "sold," or at a minimum licensed, by the start-up to Local Grocer. Does that claim, plausible (if not quite persuasive) as it is, mean Local Grocer did not agree to the email being sent? Surely not. Common sense, then, coupled with plaintiffs' omission of any caselaw charting a contradictory course, disposes of the "consent-upon-consent" theory. On the pleadings, developers consented to Google's collection of plaintiffs' data— irrespective of plaintiffs' impression of, and engagement with, the WAA feature.

C. "Secret Scripts"

As discussed, the FAC threads its focus on GA for Firebase with allegations of "secret scripts" executing a covert GA for Firebase program, undetectable to anyone but Google. Because those allegations are of fraud, they are "subject to Rule 9(b)'s heightened pleading requirement," and "must be accompanied by 'the who, what, when, where, and how' of the misconduct charged." *See Vess v. Ciba-Geigy Corp. USA,* 317 F.3d 1097, 1104 (9th Cir. 2003) (internal quotation marks and citation omitted); *id.* at 1106 (quoting *Cooper,* 137 F.3d at 627). On this score, plaintiffs come up decidedly short. Canvassing the FAC, one searches in vain for when the "secret scripts" plot was hatched; which Google departments (let alone employees) were involved; and anything resembling a particular date, time, or place. *See Vess,* 317 F.3d at 1107 (citations omitted). Nor were these factual gaps filled in at oral argument, where plaintiffs' counsel carefully walked back the FAC's most sensational accusation. *Compare* FAC ¶ 3, Dkt. 60 at 5 ("Google

[7] There is, of course, a "having it both ways" quality to this hypothetical: whereas plaintiffs depict users as effectively incapable of looking beyond the four corners of any one Google policy, developers supposedly are sensitive to every inch of Google's vast operating landscape.

surreptitiously collected . . . data using secret software scripts embedded in Google's Firebase SDK platform."), *with* Tr., Dkt. 98 at 39 ("[T]here *may be* . . . a . . . violation here, which is that Google just simply doesn't *adequately disclose* to people that it has this embedded Firebase SDK script[.]") (emphasis added). In short, plaintiffs' "secret scripts" story is woefully underdeveloped. It wilts under Rule 9(b) scrutiny, and has no bearing on the claim-specific analysis below.

D. Claims for Relief

Google's motion fails as to plaintiffs' claims under § 631 of CIPA, the CDAFA, intrusion upon seclusion, and invasion of privacy. Conversely, plaintiffs' allegations do not establish entitlement to relief under the Wiretap Act, § 632 of CIPA, and the UCL.

1. Wiretap Act

Plaintiffs' first claim for relief invokes § 2511(1)(a) of the Wiretap Act, which "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.'" *Backhaut v. Apple Inc.,* 148 F.Supp.3d 844, 849 (N.D. Cal. 2015) (quoting 18 U.S.C. § 2511(1)(a)), *aff'd*, 723 F.App'x 405 (9th Cir. 2018). Relevant here, "the consent of one party is a complete defense to a Wiretap Act claim[.]" *In re Yahoo Mail Litigation,* 7 F.Supp.3d 1016, 1026 (N.D. Cal. 2014) (citation omitted). Because Google's alleged interceptions occurred with the consent of app developers, plaintiffs do not make out a § 2511(1)(a) violation.[8] *See supra* Part IV.B.

2. CIPA

California's CIPA statute, enacted in 1967 to confront "the development of new devices and techniques for the purpose of eavesdropping," serves to "protect the right of privacy" of the

[8] Plaintiffs' fallback argument, grounded in the crime-tort exception to the Wiretap Act's consent defense, is unavailing. "Alleged interceptions fall within the tort or crime exception only where 'the primary motivation or a determining factor in the interceptor's actions has been to injure plaintiffs tortiously,' . . . [and] cannot apply where the interceptor's 'purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money.'" *In re Google Inc. Gmail Litigation*, 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014) (bracketing omitted) (quoting *In re DoubleClick Inc. Privacy Litigation*, 154 F.Supp.2d 497, 518 (S.D.N.Y. 2001)).

state's citizenry. Cal. Penal Code § 630. Plaintiffs allege violations of sections 631 and 632 of CIPA, which proscribe wiretapping and eavesdropping, respectively.

"Section 631 of CIPA makes it unlawful to use 'any machine, instrument or contrivance' to intentionally intercept the content of a communication over any 'telegraph or telephone wire, line, cable or instrument,' or to read, attempt to read, or learn the 'contents[9] or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable' without the consent of all parties to the communication." *In re Yahoo Mail Litigation,* 7 F.Supp.3d at 1036 (quoting Cal. Penal Code § 631(a)). Plaintiffs—as parties to communications that were intentionally intercepted without their consent—state a viable § 631 basis for relief. *See supra* Part IV.A.

Plaintiffs' § 632 argument, by contrast, fares decidedly worse. "Section 632 does not prohibit eavesdropping in general," but rather "the use of any electronic amplifying or recording device to eavesdrop upon or record a confidential communication." *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) (internal quotation marks and citation omitted). In order for a conversation to be "confidential under section 632," at least one party to the conversation must carry "an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan v. Flanagan,* 27 Cal.4th 766, 776-77 (2002). Significantly, the California courts "have developed a presumption that [i]nternet communications do not reasonably give rise to that expectation." *See Revitch,* 2019 WL 5485330, at *3 (collecting cases).

Here, plaintiffs, pointing to the WAA Materials, plausibly demonstrate an "objectively reasonable expectation" that their communications with third-party apps would not be "recorded" by Google; but that expectation, fair as it is, does not reasonably give rise to the expectation that *nobody* (including the apps' developers) would record the communications. *Flanagan,* 27 Cal.4th

[9] Google foregoes any argument that the data collected by GA for Firebase does not reach the "contents" of users' communications with third-party apps.

United States District Court
Northern District of California

at 777. To make out the latter showing, plaintiffs must plead unique, definite circumstances rebutting California's presumption against online confidentiality. Because they have not done so, the § 632 prong of their CIPA claim is dismissed.

3. <u>CDAFA</u>

"The CDAFA is California's computer abuse law." *Oracle USA, Inc. v. Rimini Street, Inc.,* 879 F.3d 948, 960 (9th Cir. 2018), *rev'd in part on other grounds,* 139 S. Ct. 873 (2019). It states in pertinent part that an individual is "guilty of a public offense" if he or she "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network[.]" Cal. Penal Code 502(c)(2). Homing in on the CDAFA's "without permission" element, Google marshals cases in support of the proposition that a party only acts "without permission" when it "circumvents technical or code-based barriers in place to restrict or bar a user's access." *See, e.g., Facebook Inc. v. Power Ventures,* 844 F.Supp.2d 1025, 1036 (N.D. Cal. 2012) (citation omitted). Under this logic, Google could not have overcome any "code-based barriers," because Google *wrote* all the relevant code. *Id.* (citation omitted). Yet, as plaintiffs correctly note, this argument mistakes the sufficient for the necessary.

Faced with CDAFA claims, the Ninth Circuit repeatedly has emphasized that "[a] plain reading of the statute demonstrates that its focus is on the unauthorized *taking* or *use* of information." *United States v. Christensen,* 828 F.3d 763, 789 (9th Cir. 2015) (emphasis added); *see also Oracle,* 879 F.3d at 962 (quoting *Christensen*). While taking or use that occurs subsequent to unauthorized access doubtless fits this description, the same goes for authorized access which turns "unlawful [when] . . . the person 'without permission takes, copies, or makes use of' [the] data" in question. *Christensen,* 828 F.3d at 789 (quoting Cal. Penal Code § 502(c)(2)); *see also id.* (clarifying that the CDAFA "does not require *unauthorized* access," but rather "*knowing* access") (emphasis in original) (citations omitted). The raft of cases Google relies upon, which work off the premise that data accessed without permission is also, if taken, taken without permission, does not disturb this conclusion. Because plaintiffs have alleged Google's knowing access to, and unpermitted taking of, plaintiffs' app activity data, they adequately state a claim under the CDAFA.

4-5. **Invasion of Privacy**

Plaintiffs' fourth and fifth claims are 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 intruded into a place, conversation, or matter as to which the plaintiff had a reasonable expectation of privacy, and (2) the intrusion occurred in a manner highly offensive to a reasonable person." *In Re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 601 (9th Cir. 2020) (internal quotation marks, alterations, and citation omitted). "A claim for invasion of privacy under the California Constitution involves similar elements," requiring a plaintiff to 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 social norms such that the breach is highly offensive." *Id.* (internal quotation marks, alterations, and citation omitted). "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." *In Re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d at 601 (citation omitted).

Struggle as Google might to suggest otherwise, the Ninth Circuit's recent decision in *In re Facebook, Inc. Internet Tracking Litigation* is instructive on the viability of these two claims. There, likewise testing California claims for intrusion upon seclusion and invasion of privacy, the court considered Facebook's practice of collecting certain user data from third-party websites, even after the user had logged off Facebook, in the context of Facebook's representation that "if you log out of Facebook, we will not receive this information[.]" *Id.* at 603 (quoting Facebook's "Help Center" website). Addressing the reasonableness of the users' expectation of privacy, the court rejected Facebook's contention that plaintiffs were obliged "to identify specific, sensitive information that Facebook collected," finding instead that "*both* the nature of collection and the sensitivity of the collected information are important." *Id.* (emphasis in original). Because the data at issue comprised "browsing histories and habits"—as opposed to, say, mere IP addresses—the court found it sufficiently sensitive in nature, *id.* at 604 (distinguishing *United States v. Forrester,* 512 F.3d 500 (9th Cir. 2008)); and because "[p]laintiffs . . . plausibly alleged that Facebook set an expectation that logged-out user data would not be collected, but then collected it anyway," the court found the nature of the collection sufficiently troubling, *id.* at 602. *See also id.* at 603 (observing that, in analogous data privacy cases, "the critical fact was that the online entity represented to the plaintiffs that their information would not be collected, but then proceeded to collect it anyway"). As for the "highly offensive" issue, the court stressed the uniquely subjective nature of the inquiry, before concluding it "cannot be resolved at the pleading stage."[10] *Id.* at 606 (additionally noting that the "highly offensive analysis" is, at bottom, a "public policy" determination).

By any assessment, there is, at this early juncture, scant daylight between the allegations of *In re Facebook, Inc. Internet Tracking Litigation* and those lodged by plaintiffs here. Per the FAC, Google intercepted data akin to "browsing habits and histories," including "detailed URL requests, app browsing histories, and search queries which [p]laintiffs . . . sent to those apps[.]" *Compare id.* at 604, *with* FAC ¶ 241, Dkt. 60 at 67. These interceptions took place after Google, through the WAA Materials, "set an expectation" that it would not save plaintiffs' "activity on . . . apps . . . that use Google services" unless plaintiffs turned WAA "on." *Compare In re Facebook, Inc. Internet Tracking Litigation,* 956 F.3d at 602, *with supra* Part II.A. Nor is the offensiveness of Google's putative misconduct any less a matter of "public policy," or any more susceptible to "resol[ution] at the pleading stage," than that ascribed to Facebook. In sum, the Ninth Circuit has left little doubt as to plaintiffs' intrusion upon seclusion and invasion of privacy claims. Both survive Google's motion to dismiss.

[10] Although *In re Facebook, Inc. Internet Tracking Litigation* articulates a more nuanced—and, in some pleading-specific regards, more forgiving—conception of individual privacy expectations for purposes of intrusion upon seclusion and invasion of privacy, it explicitly declines to pass upon "the requisite elements" of a CIPA claim. 956 F.3d at 608. The decision consequently furnishes no basis to depart from the California courts' settled, presumptively-exacting approach to CIPA's "confidentiality" requirement. *See supra* Part IV.D.2.

6. UCL

Plaintiffs' final claim, for violations of the UCL, fails for lack of standing. Over and above the demands of Article III, the UCL limits standing to those who have "suffered injury in fact and lost money or property as a result of . . . unfair competition." Cal. Bus. & Prof. Code § 17204. Thus, "[t]o satisfy the narrower standing requirements imposed by [§ 17204], a party must . . . (1) establish a loss or deprivation of money or property sufficient to qualify as injury in fact . . . and (2) show that the economic injury was the result of, i.e., *caused by,* the unfair business practice . . . that is the gravamen of the claim." *Kwikset Corp. v. Superior Court,* 51 Cal.4th 310, 322 (2011) (emphasis in original). Keenly aware that no federal court has wedged individual digital data into the UCL's "money or property" box,"[11] plaintiffs emphasize the actual money they supposedly gave to Firebase apps. This approach falters on two fronts.

First, plaintiffs state that they "paid for certain apps whereby Google received money," but provide no detail concerning which apps they paid for, when, and in what amount. This is particularly problematic from a plausibility perspective because, as plaintiffs do not contest, the apps named in the FAC are free to download. Second, even if plaintiffs did transact with the apps—by, for instance, making "in-app purchases"—one struggles to imagine they did so *because of* their understanding of the apps' data practices vis-à-vis Google. Here again, the apps' "free-to-download" status rises to the fore: to the extent plaintiffs purchased in-app items or services, those purchases likely were "the result of, i.e., *caused by*," the desire to obtain said items or services. *Kwikset,* 51 Cal.4th at 322 (emphasis in original). Plaintiffs' UCL claim accordingly is dismissed.

V. CONCLUSION

Consistent with the foregoing, Google's motion is granted with respect to plaintiffs' claims for relief under the Wiretap Act, § 632 of CIPA, and the UCL. The motion is denied in all other respects. Should plaintiffs wish to file an amended complaint, they are given leave to do so within

[11] *In re Facebook, Inc. Internet Tracking Litigation,* which plaintiffs wishfully invoke (and selectively quote), dealt exclusively with "Article III standing." 956 F.3d at 600.

21 days of the issuance of this order. Upon plaintiffs' filing of an amended complaint, Google shall have 14 days to file a responsive pleading. In the event plaintiffs elect not to file an amended complaint, Google shall have 14 days following notice of such election to file an answer to the FAC.

IT IS SO ORDERED.

Dated: May 21, 2021

RICHARD SEEBORG
Chief United States District Judge