

United States District Court
Northern District of California

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

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.

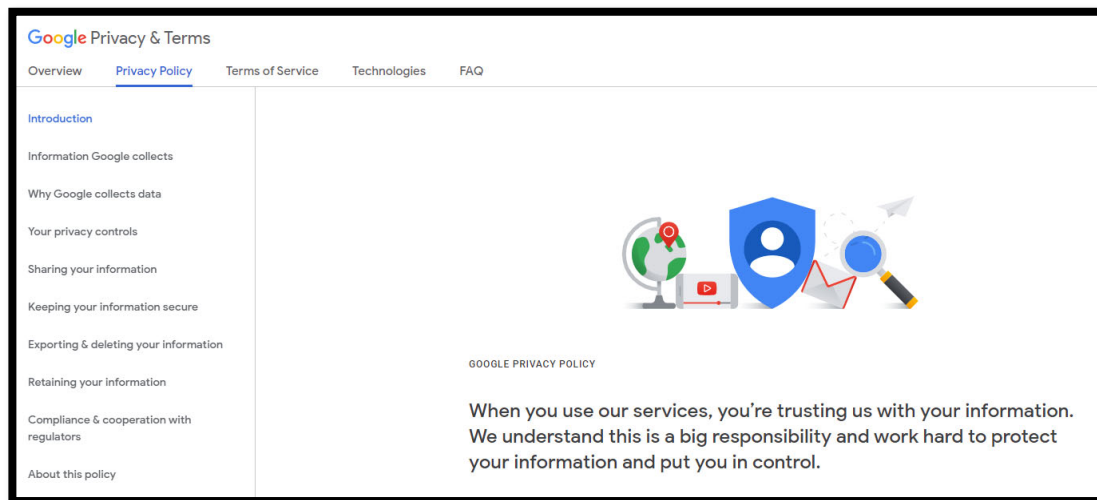
II. BACKGROUND¹

A. Google's User Privacy Framework

Google, no stranger to privacy disputes, currently maintains a complex user-facing² 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.



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.

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

...

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

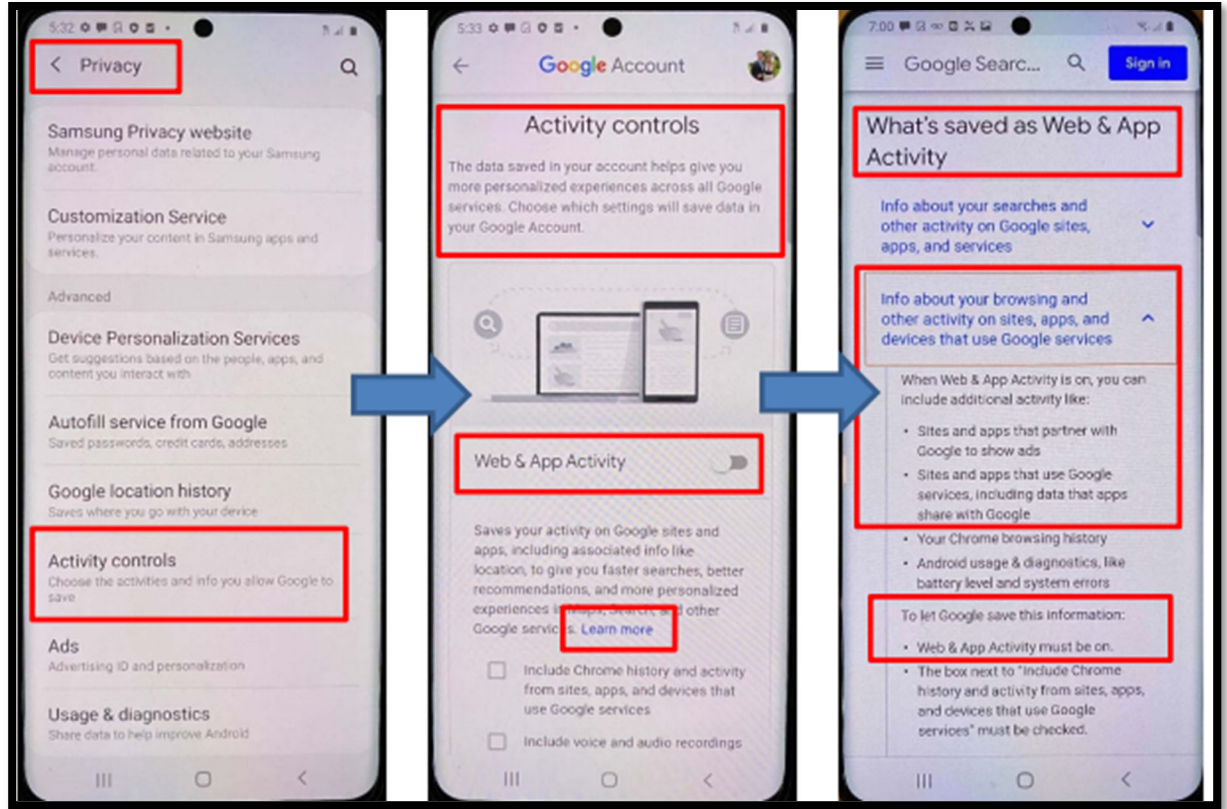
Further down the “Privacy Policy” page, under the sub-heading “Ways to review and update your information,” Google presents a hyperlink to the “My Activity” portal, which “allows you to review and control data that’s created when you uses Google services[.]” By clicking the “My Activity” hyperlink and 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.”

//
//

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



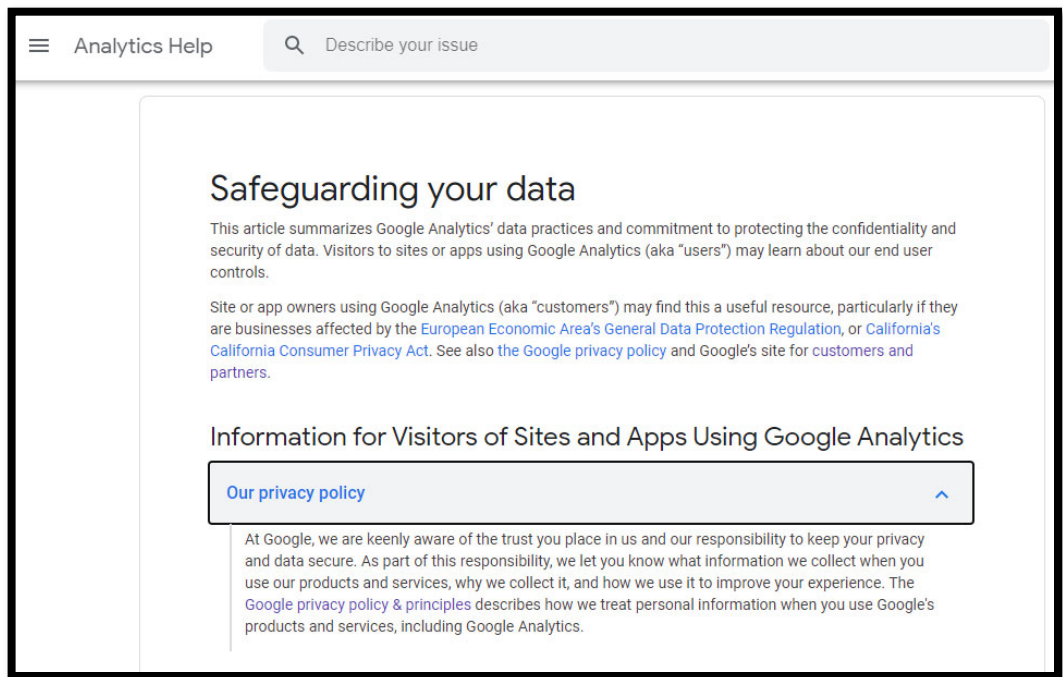
FAC ¶ 71, Dkt. 60 at 23 (displaying these screenshots). Unlike the Privacy and Terms page, the WAA Materials do not define or list “Google services.” Neither the WAA Materials nor the Privacy and Terms hub defines “Google Account.”

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”).

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



11
 12
 13
 14
 15
 16
 17
 18
 19
 20
 21
 22
 23 ³ These disclosures are catalogued in a “Help Center,” which the FAC characterizes as the “[h]elp
 24 page intended for use by app developers who use Firebase SDK.” See FAC ¶ 105, Dkt. 60 at 33.
 25 While strictly true, this characterization belies the fact that the “Help Center” is also “intended for
 26 use” by *anyone* (not just developers) who is curious about Google Analytics generally (not just
 27 GA for Firebase). Users, for instance, may access the “Help Center” from the Privacy and Terms
 28 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.

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

3 C. Alleged Misconduct

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

17 Distinct from GA for Firebase in that they are known only to Google, these “secret scripts”
18 nevertheless are, per the FAC, strikingly similar in practice to GA for Firebase. Indeed,
19 elaborating on what types of data the “secret scripts” ostensibly collect, the FAC links to a
20 webpage describing the data collection process for GA for Firebase. In this fashion, plaintiffs’
21 “secret scripts” narrative seems to distill to Google’s alleged practice of embedding a “shadow”
22 version of GA for Firebase, for its own exclusive benefit, within other of the Firebase toolkit’s
23

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

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

4 III. LEGAL STANDARD

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

14 IV. DISCUSSION

15 Plaintiffs advance six claims for relief, under (i) section 2511(1)(a) of the Wiretap Act, (ii)
 16 sections 631 and 632 of the California Invasion of Privacy Act (“CIPA”), (iii) the California
 17 Computer Data Access and Fraud Act (“CDAFA”), (iv) California’s common law right against
 18 intrusion upon seclusion, (v) California’s constitutional proscription of invasion of privacy, and
 19 (vi) California’s Unfair Competition Law (“UCL”). While claims (iii)-(v), along with the section
 20 631 component of claim (ii), withstand Google’s 12(b)(6) attack, the remainder do not. This
 21 conclusion rests in large part on three threshold determinations. As a pleading matter, plaintiffs
 22 did not consent to Google collecting their data, through GA for Firebase, with WAA turned “off”;
 23 developers did consent to such data collection; and Google has not deployed any “secret scripts.”

24 A. User Consent

25 Plaintiffs do not deny, for each app at issue, reading and agreeing to a developer-generated
 26 disclosure—made at Google’s behest—outlining the “use of the [GA for Firebase] Service . . . [to]
 27 collect[] and process[] data.” Instead, combining (i) the WAA Materials’ statement that WAA
 28

1 “must be on” in order “[t]o let Google save . . . information” concerning activity on apps “that use
2 Google services,” and (ii) the Privacy Policy’s definition of “services” as including “[p]roducts
3 that are integrated into third-party apps, like ads and embedded Google Maps,” they claim to have
4 interpreted the WAA feature as superseding those app-specific disclosures. Google counters that
5 this interpretation is too unreasonable to serve as a plausible basis for relief. For three reasons,
6 Google’s argument misses the mark.

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

23 Second, the WAA Materials’ statement that turning WAA on or off governs whether data
24 is “saved in” a user’s “Google Account” does not clearly exclude GA for Firebase from the WAA
25 feature’s operative scope. This finding follows another: the concept of a “Google Account” is, at
26 best, nebulous. Asked, for instance, to define it at the hearing for this motion, Google’s counsel
27 noted “there’s an account creation process . . . involv[ing] assigning an email address and making
28

1 certain disclosures”; acknowledged the nominal distinction between data stored by Google “in” a
 2 Google Account, when WAA is turned “on,” and data stored by Google elsewhere; and carried on
 3 with his argument. *See* Tr., Dkt. 98 at 28-31. Working off this response and other scattered
 4 descriptions of discrete Google Account *features*—as opposed to, say, a succinct, plain English
 5 explanation of what exactly a Google Account *is*—one might hazard to construe the Google
 6 Account offering as (i) a Google service available to any individual with an email address, that (ii)
 7 monitors the individual’s activity across all of Google’s user-facing services (Gmail, Chrome,
 8 Google Search, Google Maps, etc.), across all digital devices (laptop, smart-phone, tablet, etc.),
 9 and (iii) “personalizes” the individual’s experiences of those services accordingly. Yet plaintiffs’
 10 failure to grasp as much—in the absence of any guidance from the WAA Materials, Privacy and
 11 Terms portal, or any other Google resource identified in this litigation—simply cannot count
 12 against them. The average internet user is not a full-stack engineer; he or she should not be treated
 13 as one when Google explains which digital data goes into which digital buckets, and where the
 14 corresponding spigots might be found. That plaintiffs did not first perceive the precise contours of
 15 a Google Account, before arriving at their averred understanding of the WAA feature, does not
 16 doom their claims.

17 Finally, and in a related vein, Google’s gripe that plaintiffs attempt to pass WAA off as “a
 18 single valve that can control the entire flow of data on the Internet” falls on less-than-sympathetic
 19 ears. *See* Reply, Dkt. 82 at 14. As the present controversy throws into sharp relief, navigating
 20 Google’s user-facing privacy representations is a singularly fragmented affair.⁵ On the one hand,
 21

22 ⁵ Consider this: per Google, a *correct* interpretation of the WAA feature’s functionality
 23 synthesizes (i) one landing page’s statement of what happens when WAA is “on,” (ii) the
 24 preceding landing page’s mention of “your Google Account,” (iii) working knowledge of what a
 25 Google Account is (presumably drawn from a series of separate webpages), (iv) a strained reading
 26 of the Privacy Policy’s definition of “Google Services” (as provided in one of the five sections of
 27 Google’s Privacy and Terms hub), and (v) familiarity with Google’s custom of “respect[ing] the
 28 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

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

10 **B. Developer Consent**

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

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

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

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

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

13 C. “Secret Scripts”

14 As discussed, the FAC threads its focus on GA for Firebase with allegations of “secret
 15 scripts” executing a covert GA for Firebase program, undetectable to anyone but Google. Because
 16 those allegations are of fraud, they are “subject to Rule 9(b)’s heightened pleading requirement,”
 17 and “must be accompanied by ‘the who, what, when, where, and how’ of the misconduct
 18 charged.” *See Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1104 (9th Cir. 2003) (internal
 19 quotation marks and citation omitted); *id.* at 1106 (quoting *Cooper*, 137 F.3d at 627). On this
 20 score, plaintiffs come up decidedly short. Canvassing the FAC, one searches in vain for when the
 21 “secret scripts” plot was hatched; which Google departments (let alone employees) were involved;
 22 and anything resembling a particular date, time, or place. *See Vess*, 317 F.3d at 1107 (citations
 23 omitted). Nor were these factual gaps filled in at oral argument, where plaintiffs’ counsel carefully
 24 walked back the FAC’s most sensational accusation. *Compare* FAC ¶ 3, Dkt. 60 at 5 (“Google
 25

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

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

6 **D. Claims for Relief**

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

10 **1. Wiretap Act**

11 Plaintiffs’ first claim for relief invokes § 2511(1)(a) of the Wiretap Act, which “provides a
 12 private right of action against any person who ‘intentionally intercepts, endeavors to intercept, or
 13 procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic
 14 communication.’” *Backhaut v. Apple Inc.*, 148 F.Supp.3d 844, 849 (N.D. Cal. 2015) (quoting 18
 15 U.S.C. § 2511(1)(a)), *aff’d*, 723 F.App’x 405 (9th Cir. 2018). Relevant here, “the consent of one
 16 party is a complete defense to a Wiretap Act claim[.]” *In re Yahoo Mail Litigation*, 7 F.Supp.3d
 17 1016, 1026 (N.D. Cal. 2014) (citation omitted). Because Google’s alleged interceptions occurred
 18 with the consent of app developers, plaintiffs do not make out a § 2511(1)(a) violation.⁸ *See supra*
 19 Part IV.B.

20 **2. CIPA**

21 California’s CIPA statute, enacted in 1967 to confront “the development of new devices
 22 and techniques for the purpose of eavesdropping,” serves to “protect the right of privacy” of the

24 ⁸ Plaintiffs’ fallback argument, grounded in the crime-tort exception to the Wiretap Act’s consent
 25 defense, is unavailing. “Alleged interceptions fall within the tort or crime exception only where
 26 ‘the primary motivation or a determining factor in the interceptor’s actions has been to injure
 27 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)).

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

3 “Section 631 of CIPA makes it unlawful to use ‘any machine, instrument or contrivance’
4 to intentionally intercept the content of a communication over any ‘telegraph or telephone wire,
5 line, cable or instrument,’ or to read, attempt to read, or learn the ‘contents⁹ or meaning of any
6 message, report, or communication while the same is in transit or passing over any wire, line or
7 cable’ without the consent of all parties to the communication.” *In re Yahoo Mail Litigation*, 7
8 F.Supp.3d at 1036 (quoting Cal. Penal Code § 631(a)). Plaintiffs—as parties to communications
9 that were intentionally intercepted without their consent—state a viable § 631 basis for relief. *See*
10 *supra* Part IV.A.

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

21 Here, plaintiffs, pointing to the WAA Materials, plausibly demonstrate an “objectively
22 reasonable expectation” that their communications with third-party apps would not be “recorded”
23 by Google; but that expectation, fair as it is, does not reasonably give rise to the expectation that
24 *nobody* (including the apps’ developers) would record the communications. *Flanagan*, 27 Cal.4th
25

26 ⁹ Google foregoes any argument that the data collected by GA for Firebase does not reach the
27 “contents” of users’ communications with third-party apps.

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

4 3. CDAFA

5 “The CDAFA is California’s computer abuse law.” *Oracle USA, Inc. v. Rimini Street, Inc.*,
 6 879 F.3d 948, 960 (9th Cir. 2018), *rev’d in part on other grounds*, 139 S. Ct. 873 (2019). It states
 7 in pertinent part that an individual is “guilty of a public offense” if he or she “[k]nowingly
 8 accesses and without permission takes, copies, or makes use of any data from a computer,
 9 computer system, or computer network[.]” Cal. Penal Code 502(c)(2). Homing in on the
 10 CDAFA’s “without permission” element, Google marshals cases in support of the proposition that
 11 a party only acts “without permission” when it “circumvents technical or code-based barriers in
 12 place to restrict or bar a user’s access.” *See, e.g., Facebook Inc. v. Power Ventures*, 844 F.Supp.2d
 13 1025, 1036 (N.D. Cal. 2012) (citation omitted). Under this logic, Google could not have overcome
 14 any “code-based barriers,” because Google *wrote* all the relevant code. *Id.* (citation omitted). Yet,
 15 as plaintiffs correctly note, this argument mistakes the sufficient for the necessary.

16 Faced with CDAFA claims, the Ninth Circuit repeatedly has emphasized that “[a] plain
 17 reading of the statute demonstrates that its focus is on the unauthorized *taking* or *use* of
 18 information.” *United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2015) (emphasis added);
 19 *see also Oracle*, 879 F.3d at 962 (quoting *Christensen*). While taking or use that occurs
 20 subsequent to unauthorized access doubtless fits this description, the same goes for authorized
 21 access which turns “unlawful [when] . . . the person ‘without permission takes, copies, or makes
 22 use of’ [the] data” in question. *Christensen*, 828 F.3d at 789 (quoting Cal. Penal Code §
 23 502(c)(2)); *see also id.* (clarifying that the CDAFA “does not require *unauthorized* access,” but
 24 rather “*knowing* access”) (emphasis in original) (citations omitted). The raft of cases Google relies
 25 upon, which work off the premise that data accessed without permission is also, if taken, taken
 26 without permission, does not disturb this conclusion. Because plaintiffs have alleged Google’s
 27 knowing access to, and unpermitted taking of, plaintiffs’ app activity data, they adequately state a
 28

1 claim under the CDAFA.

2 **4-5. Invasion of Privacy**

3 Plaintiffs' fourth and fifth claims are for intrusion upon seclusion and invasion of privacy.
 4 "To state a claim for intrusion upon seclusion under California common law, a plaintiff must plead
 5 that (1) a defendant intentionally intruded into a place, conversation, or matter as to which the
 6 plaintiff had a reasonable expectation of privacy, and (2) the intrusion occurred in a manner highly
 7 offensive to a reasonable person." *In Re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d
 8 589, 601 (9th Cir. 2020) (internal quotation marks, alterations, and citation omitted). "A claim for
 9 invasion of privacy under the California Constitution involves similar elements," requiring a
 10 plaintiff to show "that (1) they possess a legally protected privacy interest, (2) they maintain a
 11 reasonable expectation of privacy, and (3) the intrusion is so serious as to constitute an egregious
 12 breach of social norms such that the breach is highly offensive." *Id.* (internal quotation marks,
 13 alterations, and citation omitted). "Because of the similarity of the tests, courts consider the claims
 14 together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion
 15 was highly offensive." *In Re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d at 601 (citation
 16 omitted).

17 Struggle as Google might to suggest otherwise, the Ninth Circuit's recent decision in *In re*
 18 *Facebook, Inc. Internet Tracking Litigation* is instructive on the viability of these two claims.
 19 There, likewise testing California claims for intrusion upon seclusion and invasion of privacy, the
 20 court considered Facebook's practice of collecting certain user data from third-party websites,
 21 even after the user had logged off Facebook, in the context of Facebook's representation that "if
 22 you log out of Facebook, we will not receive this information[.]" *Id.* at 603 (quoting Facebook's
 23 "Help Center" website). Addressing the reasonableness of the users' expectation of privacy, the
 24 court rejected Facebook's contention that plaintiffs were obliged "to identify specific, sensitive
 25 information that Facebook collected," finding instead that "*both* the nature of collection and the
 26 sensitivity of the collected information are important." *Id.* (emphasis in original). Because the data
 27 at issue comprised "browsing histories and habits"—as opposed to, say, mere IP addresses—the

1 court found it sufficiently sensitive in nature, *id.* at 604 (distinguishing *United States v. Forrester*,
 2 512 F.3d 500 (9th Cir. 2008)); and because “[p]laintiffs . . . plausibly alleged that Facebook set an
 3 expectation that logged-out user data would not be collected, but then collected it anyway,” the
 4 court found the nature of the collection sufficiently troubling, *id.* at 602. *See also id.* at 603
 5 (observing that, in analogous data privacy cases, “the critical fact was that the online entity
 6 represented to the plaintiffs that their information would not be collected, but then proceeded to
 7 collect it anyway”). As for the “highly offensive” issue, the court stressed the uniquely subjective
 8 nature of the inquiry, before concluding it “cannot be resolved at the pleading stage.”¹⁰ *Id.* at 606
 9 (additionally noting that the “highly offensive analysis” is, at bottom, a “public policy”
 10 determination).

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

23
 24
 25 ¹⁰ Although *In re Facebook, Inc. Internet Tracking Litigation* articulates a more nuanced—and, in
 26 some pleading-specific regards, more forgiving—conception of individual privacy expectations
 27 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.

1 **6. UCL**

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

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

21 **V. CONCLUSION**

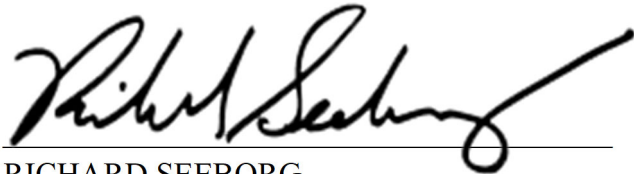
22 Consistent with the foregoing, Google’s motion is granted with respect to plaintiffs’ claims
23 for relief under the Wiretap Act, § 632 of CIPA, and the UCL. The motion is denied in all other
24 respects. Should plaintiffs wish to file an amended complaint, they are given leave to do so within
25

26 _____
27 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.

1 21 days of the issuance of this order. Upon plaintiffs’ filing of an amended complaint, Google
2 shall have 14 days to file a responsive pleading. In the event plaintiffs elect not to file an amended
3 complaint, Google shall have 14 days following notice of such election to file an answer to the
4 FAC.

5
6 **IT IS SO ORDERED.**

7
8 Dated: May 21, 2021



9
10 RICHARD SEEBORG
11 Chief United States District Judge

12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
United States District Court
Northern District of California