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 AND DENYING IN PART MOTION TO DISMISS

I. INTRODUCTION

Nine individual internet users ("plaintiffs") accuse defendant Google LLC ("Google") of violating one of the company's public-facing privacy representations. Having secured a partial dismissal of plaintiffs' First Amended Complaint ("FAC"), Google now moves to dismiss certain portions of their Second Amended Complaint ("SAC"). For the reasons set forth herein, the motion is granted in part and denied in part.

II. BACKGROUND

The parties are familiar with this controversy's full factual history, *see* Order, Dkt. 109 at 2-7 (setting it out in detail), which need not be recited here. For present purposes, three of the SAC's new averments warrant mention.

A. Breach of Contract

In lieu of plaintiffs' dismissed Wiretap Act claim, the SAC advances a state law claim for breach of contract. Like the one it replaces, this claim flows from Google's alleged practice of (i) representing, in connection with its "Web & App Activity" ("WAA") feature, that "[t]o let

Google save" information about his or her activity on "apps . . . that use Google services," a user "must" turn WAA on, while (ii) collecting such information from users who have turned WAA off.

Until at least March 2020, Google's Terms of Service explicitly incorporated Google's Privacy Policy. Google's Privacy Policy, in turn, included the following statements:

> (i) "[A]cross our services, you can adjust your privacy settings to control what we collect and how your information is used."
> (ii) "Our services include . . . [p]roducts that are integrated into third-party apps and sites, like ads[.]"
> (iii) "My Activity allows you to review and control data that's created when you use Google services . . . . Go to My Activity."
> (iv) "[W]hen you're signed in to your Google Account and have [WAA] enabled, you can get more relevant search results . . . . You can learn more here."

Two phrases within these statements—"Go to My Activity" and "learn more here"—contained hyperlinks. The "Go to My Activity" hyperlink led to a page detailing WAA and various other privacy controls. From that page, a user was two additional clicks away from the WAA Help Page, which contained this action's central alleged misrepresentation ("[t]o let Google save this information . . . Web & App Activity must be on"). The hyperlink in the second phrase, "learn more here," led directly to the WAA Help Page.

B. Data Transmission Chronology

The FAC characterized Google as transmitting users' third-party app communications to its corporate servers in real time. *See* FAC, Dkt. 60 at ¶ 49 ("Google . . . intercepts the app user's request for . . . content, surreptitiously copies that request, and then simultaneously transmits it to Google servers in California[.]"); *id.* at ¶ 245 ("The communications between Plaintiffs and apps were simultaneous to, but separate from, the channel through which Google illegally acquired the contents of those communications.") (quotation marks and emphasis omitted). The SAC, by contrast, gives this process a chronologically distinct treatment: "Google . . . intercepts the app user's request for . . . content, surreptitiously copies that request, and then *while overriding device and account level controls* simultaneously transmits the browsing data to Google servers in California[.]" SAC, Dkt. 113 at ¶ 49 (emphasis added).

C. AdMob, Cloud Messaging

The FAC charged Google with improperly collecting data in two ways: through the Google Analytics for Firebase ("GA for Firebase") product made freely available to third-party app developers as part of Google's Firebase Software Development Kit ("Firebase"),[1] and through "secret scripts" (*i.e.*, undetectable lines of software code) hidden in Firebase by Google. The SAC abandons this latter, fraud-based theory, but names two new Google services—AdMob and Cloud Messaging for Firebase ("Cloud Messaging")—as vehicles for Google's supposed misconduct:

> Google still collects data from users who turn off the "Web & App Activity" feature. Google collects this data through various backdoors made available through and in connection with Google's Firebase Software Development Kit, including not only Google Analytics for Firebase but also without limitation AdMob and Cloud Messaging[.]

SAC, Dkt. 113 at ¶ 6. Google does not dispute these services' interoperability with Firebase.

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). In other words, the complaint must contain "factual content allow[ing] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged," *Ashcroft v. Iqbal*, 556 U.S. 662, 663 (2009), and be "sufficiently detailed to give fair notice to the opposing party of the nature of the claim so that the party may effectively defend against it[.]" *Sensible Foods, LLC v. World Gourmet, Inc.*, 2011 WL 5244716, at *3 (N.D. Cal. Nov. 3, 2011) (citing *Starr v. Baca*, 633 F.3d 1191, 1204 (9th Cir. 2011)).

---

[1] *See* Order, Dkt. 109 at 4 ("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. [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.").

IV. DISCUSSION

Of the five bases for relief in the SAC, Google's motion targets two: breach of contract, and violation of section 631 of the California Invasion of Privacy Act ("CIPA"). Google additionally seeks dismissal of plaintiffs' AdMob and Cloud Messaging allegations, arguing they do not convey "what AdMob and Cloud Messaging are, or how they support [p]laintiffs' theories." *See* Mot., Dkt. 115 at 16. While Google is correct as to the breach of contract and CIPA § 631 claims, the AdMob and Cloud Messaging averments have been adequately pled.[2]

A. Breach of Contract

Plaintiffs' breach of contract claim requires them to state "(1) the existence of a contract with [Google], (2) their performance under that contract, (3) [Google] breached that contract, and (4) they suffered damages." *In re Facebook, Inc. Internet Tracking Litigation* ("*In re Facebook*"), 956 F.3d 589, 610 (9th Cir. 2020). Attempting to make this showing, plaintiffs draw on Google's Privacy Policy and the WAA Help Page. Neither document is up to the task.

1. Privacy Policy

The parties agree Google's Terms of Service is an enforceable contract that, for the brunt of the class period, incorporated Google's Privacy Policy. Consistent with this, plaintiffs mount their contractual breach claim atop a trio of Privacy Policy assertions:

> (i) "[A]cross our services, you can adjust your privacy settings to control what we collect and how your information is used."
> (ii) "Our services include . . . [p]roducts that are integrated into third-party apps and sites, like ads[.]"
> (iii) "My Activity allows you to review and control data that's created when you use Google services . . . . Go to My Activity."

Collapsing any distinction between "My Activity" (a hub containing multiple privacy controls) and WAA (one of those controls), plaintiffs insist that "a reasonable user could interpret these provisions to promise that My Activity (WAA) can be used to control the data that Google collects

[2] Because the motion is granted as to plaintiffs' breach of contract claim, there is no occasion to reach Google's fallback request to strike those portions of the SAC dealing with breach of contract damages.

through Google's services." *See* Opp'n, Dkt. 121 at 19; *see also id.* at 21 (continuing to refer to "My Activity" as "My Activity (WAA)"). Yet as Google persuasively counters, the "My Activity" hub and WAA feature *are* distinct; and even assuming the Privacy Policy text singled out by plaintiffs imposes a contractual duty, that duty relates exclusively to the former. The question thus becomes: does the alleged misconduct contravene any "My Activity"-oriented promise made by the Privacy Policy?

As a recent analogous case in this district illustrates, it does not. In *In re Google Location History Litigation*, plaintiffs similarly premised a breach of contract claim on a broadly worded provision in Google's Terms of Service ("users can adjust their privacy settings to control what Google collects and how their information is used") and an alleged misrepresentation around "the effect of [one] setting specifically." 514 F.Supp.3d 1147, 1160 (N.D. Cal. 2021) (internal quotation marks and bracketing omitted). Dismissing the claim, the court reasoned that the Terms of Service provision did "not actually bind Google to offer any particular privacy settings," and that, to the degree it extended a promise, that promise would only be broken if "[p]laintiffs . . . allege[d] that they had no control whatsoever over their privacy settings[.]" *Id.* Put briefly, the same logic applies here. At most, the Privacy Policy language identified by plaintiffs obliges Google to (i) provide users with an unspecified level of control over data created in connection with an unspecified number of Google services, and (ii) maintain a "My Activity" hub to that end. Because the SAC omits facts permitting the inference that Google neglected this obligation, plaintiffs cannot rely on the "My Activity" Privacy Policy language to sustain a claim for breach of contract.

2. WAA Help Page

Plaintiffs' alternative effort to come up with a contractual violation, by holding out the WAA Help Page as either its own contract or the incorporated part of another, fares no better. First, regarding the notion that the WAA Help Page functions as an independently enforceable agreement, plaintiffs do not allege their having secured that document's terms with valid consideration. Nor can they; as the Ninth Circuit has made clear, "[f]or a contract to exist" in this

context, the document needs to "outline shared commitments to which users must abide." *In re Facebook*, 956 F.3d at 610. That the WAA Help Page fails to do so (indeed, it asks *nothing* of users) precludes it from functioning as a standalone contract, plaintiffs' appeal to an unstated bargain for "user retention" and "goodwill" notwithstanding.[3]

Second, the WAA Help Page is not incorporated by reference into the Privacy Policy, and therefore may not benefit from the Privacy Policy's incorporation into the Terms of Service. Under California law, "[t]o properly incorporate another document, the document 'need not recite that it incorporates another document, so long as it guides the reader to the incorporated document.'" *Id.* (quoting *Shaw v. Regents of the Univ. of Cal.*, 58 Cal.App.4th 44, 54 (1997)) (bracketing omitted). While this standard is by no means exacting, it does compel the primary document to at least reference the document sought to be incorporated. *See, e.g., id.* ("The [primary document] does not reference [the incorporated document] and thus, it does not guide the reader to the incorporated document[.]"); *see also In re Holl*, 925 F.3d 1076, 1084 (9th Cir. 2019) ("[T]he incorporation is valid—and the terms of the incorporated document are binding—*so long as* the incorporation is 'clear and unequivocal, the reference is called to the attention of the other party and he consents thereto, and the terms of the incorporated document are known or easily available to the contracting parties.'") (emphasis added) (bracketing omitted) (quoting *Shaw*, 58 Cal.App.4th at 54). Here, the Privacy Policy, via its "learn more here" language, links to the WAA Help Page; but it nowhere *references* the WAA Help Page. As the absence of any caselaw holding the mere fact of a hyperlink[4] sufficient for incorporation confirms, California law requires more. All told, then, and like the Privacy Policy, the WAA Help Page affords plaintiffs no basis to state a viable claim for breach of contract.

---

[3] This conclusion holds whether the WAA Help Page is tested as an express or implied contract. *See* 1 Witkin, Summary of California Law, Contracts § 102 ("The distinction between express and implied in fact contracts relates only to the manifestation of assent; both types are based upon the expressed or apparent intention of the parties."). Approached from any angle, the WAA Help Page's offer is, on these pleadings, gratuitous.

[4] As opposed to a hyperlink embedded within language signifying the linked material—*e.g.*, "learn more by visiting the WAA Help Page."

B. CIPA § 631

The SAC's CIPA § 631 claim is likewise deficient. "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 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 1016, 1036 (N.D. Cal. 2014) (quoting Cal. Penal Code § 631(a)). The problem for plaintiffs is with the phrase "while the same is in transit": whereas the FAC alleged Google simultaneously copied and acquired users' third-party app communications, the SAC replaces that specific simultaneity with simultaneity between post-copying conduct and the data's transmission to Google. *Compare* FAC, Dkt. 60 ¶ at 49 ("Google . . . copies that request, and then simultaneously transmits it to Google servers[.]"), *with* SAC, Dkt. 113 at ¶ 49 ("Google . . . copies that request, and then while overriding device and account level controls simultaneously transmits the browsing data to Google servers[.]"). Trying to pass this artful addition to the pleadings off as some sort of typographical error, plaintiffs posit that they "could amend their complaint to add back in" the requisite § 631 simultaneity. Insofar as it echoes plaintiffs' assurance, proffered in opposition to Google's last motion to dismiss, that they could salvage their since-abandoned "secret scripts" theory, this suggestion is not well taken. The operative complaint, as plaintiffs have drafted it, does not allege Google's interception of user communications "while the same [are] in transit" to third-party apps. *See* Cal. Penal Code § 631(a). Plaintiffs' CIPA § 631 claim is consequently dismissed.

C. AdMob, Cloud Messaging

Plaintiffs' AdMob and Cloud Messaging averments, however, are well pled. The SAC provides, in relevant part, that "backdoors" in Firebase facilitate Google's illicit data collection, and that the interaction of Firebase with GA for Firebase, AdMob, and Cloud Messaging contributes to this arrangement. *See* SAC, Dkt. 113 at ¶ 6. Of course, there is no denying Google's position that by "throwing in two other products," this aspect of the SAC expands the scope of

discovery. What it does not do, though, is somehow deprive Google of the "fair notice . . . of the nature of the claim" needed "to effectively defend against it[.]" *See Sensible Foods, LLC*, 2011 WL 5244716, at *3. Nor, despite Google's protestations, does Rule 8 predicate plaintiffs' opportunity to locate wrongdoing within a given Google service upon their ability to explain that service's innermost workings to Google. There is accordingly no cause to dismiss the SAC's AdMob and Cloud Messaging allegations.

V. CONCLUSION

Consistent with the foregoing, Google's motion is granted as to the SAC's breach of contract and CIPA § 631 claims, and denied as to the allegations involving AdMob and Cloud Messaging in the SAC's three remaining claims (violation of CDAFA, invasion of privacy, and intrusion upon seclusion).[5] Should plaintiffs wish to amend their two dismissed claims, they are given leave to do so in a manner strictly honoring the duty to litigate in good faith. Any amended complaint must be filed within 14 days of the issuance of this order.

IT IS SO ORDERED.

Dated: August 18, 2021

RICHARD SEEBORG
Chief United States District Judge

[5] The pending administrative motions to file certain materials under seal, *see* Dkts. 112, 120, are denied pursuant to Local Rule 79-5(e)(1).