UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

PATRICK CALHOUN, ET AL.

Plaintiffs,

v.

GOOGLE, LLC,

Defendant.

CASE NO. 4:20-cv-05146-YGR

ORDER GRANTING IN PART AND DENYING IN PART GOOGLE'S MOTION TO DISMISS DORMANT CLAIMS

Re: Dkt. No. 1127

Pending before the Court is defendant Google LLC's motion to dismiss six of plaintiffs' claims that the court previously set aside (the "Dormant Claims") in this data privacy action. Those claims include: (1) violation of the Wiretap Act (interception); (2) invasion of privacy; (3) quasi-contract; (4) violation of the California Comprehensive Computer Data Access and Fraud Act ("CDAFA"); (5) punitive damages; and (6) declaratory relief. Having carefully considered the papers submitted and the pleadings in this action, and for the reasons set forth below, the Court **GRANTS IN PART** and **DENIES IN PART** Google's motion to dismiss.

I. BACKGROUND

A. FACTUAL BACKGROUND

The parties are familiar with the facts of this case. The Court includes in this Order only those facts that are relevant to its decision.

Plaintiffs are Google account holders who use Google's internet browser Chrome. (First Amended Complaint ("FAC") ¶ 1.) Google offers a feature called "Sync" that stores a user's personal information, including bookmarks, passwords, contacts, browsing data, and payment cards in the user's Google account. Each plaintiff elected "not to 'Sync' their browsers with their

Google accounts while browsing the web." (*Id.*) Plaintiffs claim that Google expressly promised that "[t]he personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google Account by turning on sync[.]" (*Id.* ¶ 2.) Supposedly unbeknownst to plaintiffs, Chrome collected and transmitted to Google the following data: "IP addresses linked to user agents"; "[u]nique, persistent cookie identifiers including the Client ID"; "[u]nique browser identifiers called X-Client Data Headers"; and "[b]rowsing history" which includes "GET requests" and "POST communications." (*Id.* ¶¶ 3, 52, 141.)

Google collected and transmitted plaintiffs' information through "Google source code and Chrome browser-generated re-directions." (*Id.* ¶ 137.) Plaintiffs allege that "Google instructs developers to place its source code that commands Chrome to contemporaneously re-direct the contents of the communication exchanged between the user and the website to Google in the website's header." (*Id.* ¶ 130.) Google then uses the data "to create detailed dossiers about [an] individual's personal information" for targeted advertising. (*Id.* ¶ 258.)

B. PROCEDURAL HISTORY

Although plaintiffs filed their initial complaint against Google—which advanced sixteen claims—on July 27, 2020, Judge Koh directed the parties to select ten claims (five each) to litigate. (Dkt. No. 51.) Judge Koh anticipated that after the parties litigated those claims through trial, "the Court and the parties [would] discuss what to do about the remaining [six] claims." (*Id.*)

The parties selected ten claims under Judge Koh's order, six of which survived a motion to dismiss. The claims proceeded through discovery and survived a motion for summary judgment. The Court denied plaintiffs' motion for class certification, however, finding that individualized issues of consent would predominate. (Dkt. No. 1105.) Plaintiffs resolved to proceed with their claims individually and now seek to revive the six Dormant Claims. (Dkt. Nos. 1112, 1117.) Google now moves to dismiss each of those claims. (Dkt. No. 1127.)

II. LEGAL STANDARD

A motion to dismiss under Rule 12(b)(6) tests the legal sufficiency of the claims alleged in the complaint. *Ileto v. Glock, Inc.*, 349 F.3d 1191, 1199–200 (9th Cir. 2003). The standard is well known and not in dispute.

III. DISCUSSION

The Court addresses Google's motion as to all six Dormant Claims: (a) violation of the Wiretap Act; (b) invasion of privacy; (c) quasi-contract; (d) violation of the CDAFA; (e) punitive damages; and (f) declaratory relief.

A. Wiretap Act

Google argues that plaintiffs' Wiretap Act claim based on an interception theory[1] should be dismissed for three reasons. *One*, the Wiretap Act is a one-party-consent statute, and website developers that placed Google source code within their website consented to Google's interception. *Two*, Google received plaintiffs' data in the ordinary course of business and is therefore exempt from the Wiretap Act. *Three*, plaintiffs fail to allege that Google intercepted the contents (i.e. the intended message) of plaintiffs' communications.

1. Website Developer Consent

To analyze whether the Wiretap Act immunizes Google from liability because website developers—i.e. parties to the communication—consented to Google's receipt of plaintiffs' data, the Court begins with the statute.

The Wiretap Act prohibits the intentional interception of wire, oral, or electronic communication. 18 U.S.C. § 2511(1)(a). The Act exempts from liability communications where "at least one party to the communication has given prior consent." *Pyankovska v. Abid*, 65 F.4th 1067, 1075 (9th Cir. 2023) (citing 18 U.S.C. § 2511(2)(c)–(d)). Consent is "an affirmative defense for which [the] defendant bears the burden of proof." *Calhoun v. Google LLC*, 113 F.4th 1141, 1147 (9th Cir. 2024) (citing *Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1044 (9th Cir. 2017)). Consent "can be [express] or implied, but any consent must be actual." *Id.* For "consent to be actual, the disclosures must 'explicitly notify' users of the conduct at issue." *Id.* Courts apply a reasonable person standard to determine consent. *Id.* at 1147–48.

Google argues that website developers "plainly consented" to Google receiving plaintiffs' data because website developers intentionally install Google code, which in turn routes plaintiffs'

[1] The prior Wiretap Act claim was based on an unauthorized disclosure theory. *Calhoun v. Google LLC ("Calhoun I")*, 526 F.Supp.3d 605, 617 (N.D. Cal. 2021).

data to Google, so that developers may obtain the benefit of Google's services. Because website developers elected to install the code, Google maintains that the Court may presume consent. That argument fails at the threshold on a motion to dismiss for at least three reasons.

First, Judge Koh already rejected a similar argument from Google in the first round of motion to dismiss briefing in this case. *Calhoun I*, 526 F.Supp.3d at 623–24 ("Google has not established that websites consented to, or even knew about, the interception of the subset of their communications that are with users who use Chrome without sync.")[2] Without additional factual allegations that demonstrate actual consent, the Court will not depart from Judge Koh's sound reasoning.

Second, Google's argument depends on alleged facts outside of the operative complaint. Google's citations to paragraphs 129, 130, and 140 do not support its conclusion. Paragraphs 129 and 140 describe the development and use of Google source code, while paragraph 130 alleges that "Google instructs developers to place its source code that commands Chrome to contemporaneously re-direct the contents of the communication exchanged between the user and the website to Google in the website's header." None set forth facts that suggest that website developers were informed that Google would intercept the data and then *actually* consented, implicitly or explicitly, to those terms. In fact, plaintiffs do not allege anything whatsoever about Google's communications with website developers. Summary judgment may reveal a different outcome, but the Court will not reach that conclusion on a motion to dismiss.

Third, the cases Google cites cut the other way. In *Rodriguez v. Google*, for example, the court dismissed the Wiretap Act claim where third-party application developers consented to Google's interception of personal data by using Google's application development toolkit. *Rodriguez v. Google LLC*, 2021 WL 2026726, at *2–3 (N.D. Cal. May 21, 2021). Unlike here, in

[2] Google attempts to undermine Judge Koh's reasoning by explaining that "Chrome without sync" is "just Chrome" does not affect the ultimate analysis. Although Google argues that plaintiffs used Chrome in its default state and were not required to affirmatively "opt in" to a service (like Incognito at issue in *Brown*), plaintiffs claim that Google represented to them that it would not track any personal information unless plaintiffs opted-in to sync. Judge Koh, for her part, likely would have reached the same conclusion that Google failed to establish that website developers consented to, or knew about, the interception, even in Google's default state.

Rodriguez, the plaintiffs alleged that Google requested that developers affirmatively consent to Google's data collection and that developers disclose that collection to their users. *Id.* In light of those allegations, the *Rodriguez* plaintiffs conceded that the developers knowingly agreed to Google's terms, and the court concluded that the developers had thus consented to the collection of plaintiffs' data. *Id.* at *5–6. Moreover, Google's attempt to point to the court's "consent-upon-consent" analysis misses the mark because in *Rodriguez*, the court was asked to scrutinize the developers' understanding of its users' interpretation of Google's policy, one step beyond the threshold issue raised here. *Id.* Nor does *In re Nickelodeon Consumer Privacy Litigation*, an out-of-circuit authority, help Google. There, Google explicitly contracted with Viacom to place advertisements on Viacom's website and "third-party cookies on the computers of persons who visit those websites." 827 F.3d 262, 269 (3d Cir. 2016). No similar allegations were pled in this action.

Google also cites an order denying a motion for preliminary injunction in the *In re Meta Pixel Healthcare Litigation* to support its one-party consent argument. 647 F.Supp.3d 778, 796 (N.D. Cal. 2022). Google ignores, however, that on a later motion to dismiss the court *denied* Google's efforts to dismiss the Wiretap Act claim based on developer consent because "Meta has not pointed to anything [the court] can judicially notice on this motion to dismiss to show as a matter of law that the healthcare providers did not just presumably but actually consented to the sending of sensitive healthcare information of its customers." *Doe v. Meta Platforms, Inc.*, 690 F.Supp.3d 1064, 1078 (N.D. Cal. 2023).

Based on the allegations as pled, Google cannot show that website developers consented to Google's alleged interception. Because Google does not establish developer consent as a threshold requirement, the Court need not address Google's remaining arguments on this point.

2. Data Received in the Ordinary Course of Business

Google next argues that plaintiffs' Wiretap Act claim fails because Google received plaintiffs' data in the ordinary course of business. The Wiretap Act precludes liability for any interception based on the use of "any telephone or telegraph instrument, equipment or facility, or any component thereof . . . being used by a provider of wire or electronic communication service

in the ordinary course of its business." 18 U.S.C. § 2510(5)(a)(ii). "[T]he ordinary course of business exception is narrow . . . and offers protection from liability only where an electronic communication service provider's interception facilitates the transmission of the communication at issue or is incidental to the transmission of such communication." *Brown v. Google LLC ("Brown I")*, 525 F.Supp.3d 1049, 1072 (N.D. Cal. 2021). Google argues that its source code is designed "to command [] Chrome to *contemporaneously* redirect the precise content of the GET or POST part of the communication to Google." (FAC ¶ 129) (emphasis supplied.) According to Google, any interception of plaintiffs' data thus occurs in the ordinary course of Google's advertising and analytics business.

This Court rejected a similar argument from Google in *Brown I*.[3] There, like here, Google urged the court to apply the "ordinary course of business" exception because there was a "nexus between the need to engage in the alleged interception" and Google's advertising and analytics business. *Brown I*, 525 F.Supp.3d at 1072. Judge Koh disagreed with Google's argument because it lumped together two contemporaneous communications. *Id.* The communication at issue was the communication that Google allegedly intercepted (i.e. the communication between plaintiff and the website), whereas any contemporaneous or additional communication between the website and Google was deemed unrelated. *Id.* Judge Koh reasoned that "Google's argument to the contrary would vastly expand the ordinary course of business exception by permitting electronic communication services to claim that an interception is in the ordinary course of business when it facilitates another, unrelated communication." *Id.* This Court followed Judge Koh's reasoning in denying summary judgment in *Brown.* ("*Brown II*"), 685 F.Supp.3d 909, 934–35 (N.D. Cal. 2023) ("That the second GET request is essential for Google's services, like Analytics, to work and is therefore core to Google's advertising business is tangential, at best, to whether it is necessary to 'facilitate a transmission of a communication' between a user and a third-party website.") Any remaining dispute as to the intercepting device, Chrome, or Google code's operations may be

[3] Although the facts of *Brown* are different from this case and involve a different Google product, many of the *legal* arguments that Google advanced in *Brown* overlap with those advanced in this motion.

litigated with the benefit of discovery on a motion for summary judgment. Google does not present compelling arguments to depart from that analysis now.

3. Contents of Communications

The Wiretap Act applies to only the statutorily defined content of a communication. Content includes "any information concerning the substance, purport, or meaning of [the] communication." 18 U.S.C. § 2510(8). Said differently, content means "a person's intended message to another" and does not include "record information regarding the characteristics of the message" generated in the course of the communication. *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). Google argues that plaintiffs' Wiretap Act claim must be dismissed because plaintiffs do not allege that it intercepted plaintiffs' "intended message" but rather generalized information about plaintiffs' computers, browsers, internet connections, or browsing activity.

Once again, the Court rejected a similar argument from Google in *Brown II* as to GET requests.[4] There, the Court determined that the contents of the communications included "the users' IP addresses, referers, user-agents, HTTP requests, users' actions on a website, and their search queries." 685 F.Supp.3d at 935. Although some data in that list was considered "record information" of the communication, the Court noted that full-string detailed URLs, "by virtue of including the particular document within a website that a person views, reveal much more information . . . divulg[ing] a user's personal interests, queries, and habits." *Id.* (citing *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 605 (9th Cir. 2020)). Because plaintiffs allege that Google intercepts browsing history, including GET requests which include full-string URLs (FAC ¶¶ 143–52, 161–66, 175–80), the Court will not dismiss plaintiffs' Wiretap Act claim for failure to intercept the contents of a communication. Google's factual arguments as to whether the full-string URL contains search terms cannot be resolved on a motion to dismiss.

Accordingly, the Court **DENIES** Google's motion to dismiss the Wiretap Act claim.

---

[4] "When an individual internet user visits a web page, his or her browser sends a message called a 'GET request' to the web page's server. The GET request serves two purposes: it first tells the website what information is being requested and then instructs the website to send the information back to the user. The GET request also transmits a referer header containing the personally-identifiable URL information." *Calhoun v. Google LLC ("Calhoun II")*, 113 F.4th 1141, 1144 n.2 (9th Cir. 2024).

B. Invasion of Privacy

Google next moves to dismiss plaintiffs' invasion of privacy claim—notwithstanding that plaintiffs' claim for intrusion upon seclusion survived both motions to dismiss and for summary judgment.

"[A] plaintiff alleging an invasion of privacy in violation of the state constitutional right to privacy must establish each of the following: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." *Hill v. Nat'l Collegiate Athletic Ass'n.*, 7 Cal. 4th 1, 39–40 (1994).[5] A claim for invasion of privacy is similar to a claim for intrusion upon seclusion, so courts "consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *Brown I*, 525 F.Supp.3d at 1076 (citing *Facebook Tracking*, 956 F.3d at 601). Google maintains that plaintiffs' invasion of privacy claim should be dismissed because plaintiffs fail to allege both of those elements. The Court addresses each.

1. Reasonable Expectation of Privacy

To determine whether a plaintiff has a reasonable expectation of privacy in their data, "the relevant question here is whether a user would reasonably expect that [Google] would have access to the . . . data." *Facebook Tracking*, 956 F.3d at 602. Plaintiffs argue that they would not expect that Google would have access to their data because Google represented that it would not collect their data unless the plaintiffs turned on sync.

Judge Koh previously rejected the same argument from Google reasoning that plaintiffs' allegations that (i) "Google was surreptitiously collecting the same type of data through the same process that was at issue in *Facebook Tracking*" and (ii) "Google's representations regarding Chrome's sync function could have led users to assume that Google would not receive the personal information" were sufficient to state a reasonable expectation of privacy. *Calhoun I*, 526 F.Supp.3d at 629–30. That reasoning still holds true.

[5] Google also argues, in cursory fashion, that plaintiffs' invasion of privacy claim based on the California constitution should not apply to any plaintiffs who are not residents of California. In making this argument, Google does not address that it is based in the California or the alleged conduct, and harm, likely occurred in California.

2. Serious or Highly Offensive Invasion of Privacy

"Determining whether a defendant's actions were 'highly offensive to a reasonable person' requires a holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive." *Facebook Tracking*, 956 F.3d at 606. "[T]he highly offensive analysis focuses on the degree to which the intrusion is unacceptable as a matter of public policy." *Id.* Given the factually intensive nature of the inquiry, "[c]ourts are generally hesitant to decide claims of this nature at the pleading stage." *In re Meta Pixel Healthcare Litig.*, 647 F.Supp.3d 778, 799 (N.D. Cal. 2022).

Here again, Judge Koh rejected Google's argument that its interceptions were routine and consistent with tracking practices and thus could not satisfy the element. The court concluded that while "'tracking cookies are routine,'" "[b]ased on the pled facts, a reasonable factfinder could indeed deem Google's conduct 'highly offensive.'" *Calhoun I*, 526 F.Supp.3d at 631.

Google's argument that intervening caselaw changes the legal landscape does not compel a different result. Google first relies on *Thomas v. Papa John's.* 2025 WL 1704437 (9th Cir. June 18, 2025). There, in a nonprecedential memorandum disposition, the Ninth Circuit determined that Papa John's tracking was not highly offensive because a defendant cannot "eavesdrop" on its own communication. *Id.* Google is not a party to any communication here. Google next overreads *Popa v. Microsoft*, 153 F.4th 784 (9th Cir. 2025), another opinion upon which it relies. In *Popa*, an opinion primarily analyzing standing, the Ninth Circuit mentioned in passing that the plaintiff had not explained how tracking her interactions with a website was similar to the "highly offensive" conduct required for common-law privacy torts. *Id.* at 791. Unlike this case, *Popa* did not involve secret or deceptive data collection, which is at the core of what plaintiffs allege makes Google's conduct "highly offensive." The same is true for *Hammerling v. Google*. 615 F.Supp.3d 1069, 1090 (N.D. Cal. 2022). The *Hammerling* court explained that "conduct is more likely to be 'highly offensive' where the defendant 'surreptitious[ly]' collects sensitive information" particularly where the at-issue privacy policies could reasonably be read to suggest the opposite. *Id. Hubbard v. Google* likewise was "not a case involving secret or deceptive data collection" or "plus factors"

to "elevate [Google's] conduct beyond the level of routine commercial behavior" and is therefore not persuasive. 2024 WL 3302066, at *7 (N.D. Cal. July 1, 2024). None of Google's supposedly intervening cases alter the Court's prior ruling.

In sum, the Court **DENIES** Google's motion to dismiss plaintiffs' invasion of privacy claim.

C. Quasi-Contract

For quasi-contract claims, a court implies a contract where "a defendant has been unjustly conferred a benefit through mistake, fraud, coercion, or request." *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015). "At the pleading stage, a plaintiff may alternately bring both a breach of contract claim and a quasi-contract claim—so long as the plaintiff pleads facts suggesting that the contract may be unenforceable or invalid." *In the Black Res., LLC v. Blitz Design, Inc.*, 2022 WL 17082372, at *6 (N.D. Cal. Nov. 17, 2022) (cleaned up); *Brodsky v. Apple Inc.*, 445 F.Supp.3d 110, 133 (N.D. Cal. 2020) (a "plaintiff may not plead the existence of an enforceable contract and simultaneously maintain a quasi-contract claim unless the plaintiff also pleads facts suggesting that the contract may be unenforceable or invalid.") In such cases, a "quasi-contract claim for restitution may be brought 'until it is determined whether a valid express contract exists.'" *Khan v. Brooklyn Bedding LLC*, 2025 WL 829587, at *3 (N.D. Cal. Feb. 21, 2025).

Here, plaintiffs' breach of contract claim survived a summary judgment motion. Although plaintiffs plead their quasi-contract claim in the alternative, they do not allege that the contract is invalid or unenforceable.

Accordingly, the Court **GRANTS** Google's motion to dismiss the quasi-contract claim without leave to amend. Because plaintiffs will proceed with a breach of contract claim, the Court determines that any leave to amend would be futile.

D. CDAFA

Google next moves to dismiss plaintiffs' CDAFA claim. The CDAFA imposes liability on any person who "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system,

or computer network." Cal. Penal Code § 502(c)(2). Plaintiffs allege that Google violates the CDAFA by "knowingly and without permission accessing, taking and using Plaintiffs' and the Class Members' personally identifiable information." (FAC ¶ 386.) Google disputes that plaintiffs establish that it (i) acted without permission and (ii) accessed plaintiffs' data.

Without Permission. With respect to whether Google accessed each plaintiff's computer or network "without permission," Google argues that plaintiffs did not allege that Google circumvented any technical code or barrier to receive the data in acting "without permission."

Google's position is too restrictive. Like Google acknowledges, and as the Court has already explained in *Brown*, a plaintiff may state a CDAFA claim where "a software system was designed in such a way to render ineffective any barriers that [the plaintiffs] must wish to use to prevent access to their information." *Brown I*, 525 F.Supp.3d at 1075; *Brown II*, 685 F.Supp.3d at 940 n.38 (citing *United States v. Christensen*, 825 F.3d 763, 789 (9th Cir. 2015)). Plaintiffs' allegations that Google acted without consent, providing notice, or permitting plaintiffs to opt out are therefore sufficient on a motion to dismiss.

Accessing. With respect to whether Google (rather than third parties) "accessed" a computer without permission under the CDAFA, Google maintains that it is a mere passive recipient of plaintiffs' data from third parties.

Here, the CDAFA defines access as to "cause output from" the "logical, arithmetical, or memory function resources of a computer." Cal. Penal Code § 502(b)(1). Like many of Google's arguments in this motion, the Court already rejected it in *Brown II.* 685 F.Supp.3d at 939 ("Google argues it could not have accessed plaintiffs' computers as a matter of law because it is the website developers, not Google, who embed the code which directs users' browsers to send GET requests to Google servers.") Google's argument creates a triable issue of fact as to who "caused output from" plaintiffs' computers which the Court cannot resolve on a motion to dismiss. (*See* FAC ¶ 129.)

Damage. Google also argues that plaintiffs failed to allege that they suffered any damage or loss to plaintiffs by reason of the CDAFA violation.

Again, the Court rejected this same argument in *Brown II.* Although Google argued that

plaintiffs were not harmed, the Court explained that plaintiffs may have been damaged because a financial market for data exists and "the Court cannot rule, as a matter of law, that plaintiffs suffered no damage under the CDAFA." 685 F.Supp.3d at 940. *See also Rodriguez v. Google LLC*, 772 F.Supp.3d 1093, 1110 (N.D. Cal. 2025) (same). The same reasoning applies here.

The Court thus **DENIES** Google's motion to dismiss the CDAFA claim.

E. Punitive Damages

Plaintiffs concede that punitive damages are a remedy, not a cause of action. The Court therefore **GRANTS** Google's motion to dismiss any "claim" for punitive damages without leave to amend.

F. Declaratory Relief

Google finally argues that plaintiffs' declaratory relief claim should be dismissed as duplicative of plaintiffs' other claims.

"In a case of actual controversy within its jurisdiction . . . any court of the United States, upon the filing of an appropriate pleading, may declare the rights and other legal relations of any interested party seeking such declaration, *whether or not further relief is* or could be sought." 28 U.S.C. § 2201(a) (emphasis supplied). Courts have "unique and substantial discretion in deciding whether to declare the rights of litigants." *Wilton v. Seven Falls Co*., 515 U.S. 277, 286 (1995). "[D]istrict courts possess discretion in determining whether and when to entertain an action under the Declaratory Judgment Act, even when the suit otherwise satisfies subject matter jurisdictional prerequisites." *Id.* at 282.

Overlap with other claims is not, by itself, a basis to dismiss declaratory relief. The sole case that Google cites in support of its argument, *Jensen v. Quality Loan Serv. Corp.*, 702 F.Supp.2d 1183, 1188–89, n.2 (E.D. Cal. 2010), is inapposite and analyzes declaratory relief claims that are brought under *California* law. The Court will not dismiss plaintiffs' claim for declaratory relief solely because plaintiffs have alleged other causes of action.

The Court **DENIES** Google's motion to dismiss plaintiffs' claim for declaratory relief.

IV. CONCLUSION

The Court **GRANTS** Google's motion to dismiss plaintiffs' quasi-contract and punitive damages claims without leave to amend. The Court **DENIES** Google's motion to dismiss plaintiffs' Wiretap Act, invasion of privacy, CDAFA, and Declaratory Judgment claims.

Google shall file an answer to these claims within ten (10) days of this Order.

The parties shall also meet and confer and file a joint statement on next steps within ten (10) days of this Order.

This terminates Dkt. No. 1127.

IT IS SO ORDERED.

Dated: June 2, 2026

YVONNE GONZALEZ ROGERS
UNITED STATES DISTRICT COURT JUDGE

United States District Court
Northern District of California