UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ANIBAL RODRIGUEZ, et al.,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No. 20-cv-04688-RS

ORDER DENYING GOOGLE'S MOTION FOR SUMMARY JUDGMENT

I. INTRODUCTION

This is a privacy class action brought against Google LLC ("Google"). Plaintiffs are members of two sub-classes, comprising individuals with Android and non-Android mobile devices who had certain privacy-related settings switched off in their Google accounts. In the Fourth Amended Complaint ("FAC"), Plaintiffs aver that Google contravened its user-facing privacy representations regarding its Web App and Activity ("WAA") and supplemental Web App and Activity ("(s)WAA") settings, advancing three California claims: invasion of privacy under the California Constitution, common law intrusion upon seclusion, and violation of the Comprehensive Computer Data Access and Fraud Act ("CDAFA"). Google moves for summary judgment on all claims advanced by Plaintiffs in the FAC. For the reasons set forth herein, Google's motion is denied.

II. BACKGROUND

A. WAA and (s)WAA settings

The relevant technology at issue in this case is Google's WAA and, more specifically,

(s)WAA setting. The WAA button is a Google account setting that purports to give users privacy control of Google's data logging of the user's web app and activity, such as a user's searches and activity from other Google services, information associated with the user's activity, and information about the user's location and device. The (s)WAA button, which can only be switched on if WAA is also switched on, governs information regarding a user's "[Google] Chrome history and activity from sites, apps, and devices that use Google services." Disabling WAA also disables the (s)WAA button.

B. Google Analytics for Firebase

To aid third-party app developers, Google created software development kits, including Firebase and Google Mobile Ads ("GMA"). These kits are incorporated into apps by third-party app developers and allow Google to collect user data, including data regarding required fixes or updates. If an app developer seeks information about their app users' interactions with ads, they can use Google Analytics for Firebase ("GA4F"). GA4F is a free analytical tool that takes user data from the Firebase kit and provides app developers with insight on app usage and user engagement. It is integrated in 60% of the top apps. Dkt. 361-58, Expert Report of Johnathan E. Hochman ("Hochman Rep.") ¶ 2. Functionally, GA4F works by automatically sending to Google a user's ad interactions and certain identifiers regardless of a user's (s)WAA settings, and Google will, in turn, provide analysis of that data back to the app developer. GMA logs similar ad-related interactions.

Developers can customize their usage of GA4F to receive information uniquely helpful for their app development purposes and must obtain consent from end users to use GA4F. Google argues that its sole purpose for collecting (s)WAA-off data is to provide these analytic services to app developers. This data, per Google, consists only of non-personally identifiable information and is unrelated (or, at least, not directly related) to any profit-making objectives.

GA4F specifically allows app developers to track what Google coins "attributions" and "conversions." Attribution/Conversion Tracking permits Google to "(1) log the fact that it has served an ad alongside a device identifier for accounting purposes, and (2) attribute conversion

events to those ad serving records." Google argues that its practice of Attribution/Conversion Tracking does not harm users and instead involves the sharing of just critical pieces of information, namely which device triggered the conversion event, which app sent Google the information, and "other similar pieces of information."[1]

C. Pseudonymous data

When a user toggles (s)WAA off, Google purports to treat their data as "pseudonymous."[2] Google creates a randomly-generated identifier when logging a (s)WAA-off user's analytics and ads data. This identifier permits Google to recognize the particular device and its later ad-related behavior. On Android, the identifier is labeled ad ID ("ADID") and on iOS it is referred to as Identifier for Advertiser ("IDFA"). Through its software development kits, Google collects ADID or IDFA for Google's Attribution/Conversion Tracking purposes.

Another identifier that is capable of being saved by Google through GA4F is the Google Accounts and ID Administration ID ("GAIA ID"). The "GAIA ID uniquely identifies a Google account holder"—in other words, it links data collected to a specific user's Google account. Hochman Rep. ¶ 109. Google insists that it has created technical barriers to ensure, for (s)WAA-off users, that pseudonymous data is delinked to a user's identity by first performing a "consent check" to determine a user's (s)WAA settings. Specifically, GA4F logs the device's ads personalization opt-out settings. If that check yields a (s)WAA-off result, that data is logged in the "pseudonymous space" that does not contain GAIA IDs, as those correspond to a user's Google account. When this "consent check" is performed, the retrieved device IDs are encrypted.

---

[1] As an example, Google provides that "while a conversion event could be called 'in_app_purchase,' and it could contain for the app developer pseudonymous information about what the device purchased, for Google's attribution purposes, it is just the fact that the event occurred that is logged and later used to connect an ad click at Time 1 with a purchase at Time 2." Google's Motion for Summary Judgment ("Google's Mot.") at 10-11.

[2] Google uses the term "pseudonymous" throughout its motion to describe its treatment of the data it collects from (s)WAA-off users. It is not entirely clear what Google intends to denote by use of this term, but it seems to suggest the replacement of identifiable information with a contrived identifier.

Likewise, the "GAIA-keyed" space contains no identifiers that would be in the pseudonymous log. Where there is overlap, Google encrypts that data and throws away the decryption key after six days. Google's employees are also purportedly prohibited from "joining" pseudonymous and identifiable data based on internal policies. In other words, per Google, pseudonymous and identifiable data are kept separate.

D. Google's disclosures

Google insists that users knew and consented to its tracking practices. Relying on the WAA and (s)WAA disclosures, the Google Privacy Policy ("PP"), and language in Google's Privacy Portal, Google contends that it disclosed adequately the contours of the WAA and (s)WAA buttons. Specifically, it argues that users knew the WAA and (s)WAA settings controlled only whether a user's web app and activity was linked to their "personal information," which it contends is synonymous with information "saved into [the user's] Google Account" and that those settings do not cover non-personally identifiable information ("non-PII").

First, Google points to the language surrounding the WAA and (s)WAA buttons. The WAA setting is located in a Google account's <Activity Controls> page. The subheading for <Activity Controls> states that a user may "[c]hoose the activities and info [a user] allow[s] Google to save" on that page. On the actual <Activity Controls> page, where WAA is an available setting for a user to toggle on or off, Google indicates that a user may "[c]hoose which settings will save data in your Google Account." Scrolling lower, the specific language surrounding the WAA button states that switching it on "[s]aves your activity on Google sites and apps, including associated location, to give you faster searches, better recommendations, and more personalized experiences in…[various] Google services." Finally, (s)WAA, which can only be turned on if WAA is also on, "[i]ncludes Chrome history and activity from sites, apps, and devices that use Google services." Based on the subheading on the <Activity Controls> page, Google argues that a user would know turning (s)WAA on or off controlled only whether Google could save certain information "to a user's Google account."

In support of this interpretation of the phrase "saved to your Google account," Google

points to language in its PP. The PP states that when a user signs up for a Google Account, Google may "ask for personal information, like your name, email address, telephone number, or credit card to store with your account." Google's Mot. Appx. A-7 at 4. Elsewhere, Google's PP defines "personal information" as "information which you provide to us which personally identifies you, such as your name, email address, or billing information, or other data which can be reasonably linked to such information by Google, such as information with your Google account." *Id*. at 57. Non-PII is defined as "information that is recorded about users so that it no longer reflects or references an individually identifiable user." *Id*. The PP further explains that depending on a user's account settings, the user's "activity on other sites and apps may be associated with your personal information" and Google may still "share [non-PII] publicly and with our partners." *Id*. at 6-7, 11. In other words, based on Google's PP and the WAA and (s)WAA disclosures, Google contends that users should have known that any app activity data shared with third-party developers through GA4F was not covered by the WAA and (s)WAA settings because those settings controlled only whether the data was saved in a user's account.

E. The central dispute

While Google paints its practice of tracking attributions and conversion via GA4F as basic record-keeping, Plaintiffs view it as considerably less innocuous than Google portrays. This tracking, in Plaintiffs' view, contravenes Google's (s)WAA representations to users because it gathers exactly the data Google denies saving and collecting about (s)WAA-off users. Moreover, Plaintiffs insist that Google's practices allow it to personalize ads by linking user ad interactions to any later related behavior—information advertisers are likely to find valuable—leading to Google's lucrative advertising enterprise built, in part, on (s)WAA-off data unlawfully retrieved. Accordingly, Plaintiffs contend, Google should be disgorged of all its profits derived from serving any ads to (s)WAA-off users.

For its part, Google denies that any (s)WAA-off data is saved to a user's marketing profile, which precludes it from personalizing advertising to a WAA-off user. Instead, Google insists that it engages simply in unharmful and basic record-keeping of "pseudonymous" data for (s)WAA-off

users, intended to be shared with only developers through GA4F for their own analysis.

III. LEGAL STANDARD

Summary judgment is appropriate if the pleadings, discovery, and affidavits show "that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). A genuine issue of material fact is one that could reasonably be resolved in favor of the nonmoving party, and which could "affect the outcome of the suit." *Anderson v. Liberty Lobby, Inc*., 477 U.S. 242, 248 (1986). The party moving for summary judgment bears the burden of proof to "make a showing sufficient to establish…the existence of an element essential to that party's case." *Celotex Corp. v. Catrett*, 477 U.S. 317 (1986). If the movant succeeds in demonstrating the absence of a genuine issue of material fact, the burden then shifts to the nonmoving party to "set forth specific facts showing that there is a genuine issue for trial." *Id*. at 322 n.3; *see also* Fed. R. Civ. P. 56(c)(1)(B). Evidence must be viewed in the light most favorable to the nonmoving party and all justifiable inferences must be drawn in its favor. *See Anderson*, 477 U.S. at 255. It is not the task of the court to scour the record in search of a genuine issue of triable fact. *Keenan v. Allan*, 91 F.3d 1275, 1279 (9th Cir. 1996) (citation omitted). Additionally, the non-moving party has the burden of identifying, with reasonable particularity, the evidence that precludes summary judgment. *Id.* If the nonmoving party fails to make this showing, "the moving party is entitled to a judgment as a matter of law." *Celotex*, 477 U.S. at 322.

IV. DISCUSSION

Google submits several "undisputed facts" which it insists should resolve this case entirely. These facts, according to Google, reflect that its collection of WAA and (s)WAA-off data was lawful and consistent with its representations to class members. Google's Mot. at 16-17. Accepting Google's view that these facts are true and undisputed would result in this motion being granted on four grounds: first, Google secured consent from Plaintiffs for its "basic record-keeping practices." Second, the language of Google's disclosures regarding the WAA and (s)WAA settings unequivocally explained that those settings do not control Google's "non-personal record-

keeping." If the settings were ambiguous, Google insists that each Plaintiff reviewed the Privacy Policy, which defines both personal information and non-PII. Third, Google did not use this information to target or personalize ads to Plaintiffs. Finally, the above leads to the conclusion that Google's basic record-keeping practices harms no one.

A. What WAA/(s)WAA controls is ambiguous

Google does not deny that it collects (s)WAA-off data and tracks user behavior via GA4F but argues that it did so lawfully. However, the argument that users knew the WAA button controls only whether a user's app activity data is "saved to [his or her] Google account" fails to persuade.

On the <Activity Controls> page and connected interfaces, which include the WAA and (s)WAA settings and their descriptions, Google provides multiple descriptions of what the WAA and (s)WAA settings entail. Nowhere do these disclosures indicate with reasonable clarity that (s)WAA controls not whether Google will collect data about a user's app activity at all, but only whether Google will delink the collected data from the user's GAIA-ID. The various interpretations of these disclosures render them ambiguous such that a reasonable user would expect the WAA and (s)WAA settings to control Google's collection of a user's web app and activity on products using Google's services. Documents Google produced in discovery only emphasize the WAA settings' ambiguity. One such document states that "[a]ds you respond to by clicking the ad itself or buying something on the advertiser's site" constitute what is "saved as [WAA]." Dkt. 398-8 at 9. At the very least, this could reasonably suggest that a (s)WAA-off user may interpret the exact kind of data Google saves via GA4F to be precluded from Google's data logging if they switch (s)WAA off. What is meant by the (s)WAA disclosures is thus a disputed material fact.

Google's insistence that a user should have known that "saved to your Google account" denotes only personal information is unconvincing, and its reliance on the PP provides no clarity. The (s)WAA disclosures do not distinguish between personal information and non-PII, and the PP, in defining both terms, does not expressly refer to the (s)WAA settings. Even accepting that

Google's disclosures outside of the WAA/(s)WAA settings context could somehow be relied upon to provide clarity as to those settings, that is not the case here. The PP states that a user must provide Google with their personal information to create a Google account, which is then used to authenticate a user when accessing Google's services. This does not foreclose the possibility that information which is *not* associated with a user's Google account is personal information.

Moreover, Plaintiffs' interpretation of "personal information" is consistent with California law. *In re Google RTB Consumer Privacy Litigation*, 606 F. Supp. 3d 935 (N.D. Cal. 2022) is instructive. There, the court pointed to language in the California Consumer Privacy Act ("CCPA") (amended by Stats. 2023, Ch. 551, Sec. 1. (A.B. 947)), where the California legislature defined as personal information the type of data collected by GA4F. *See* 606 F. Supp. 3d at 944. Specifically, the CCPA defines personal information as that which "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," including "[g]eolocation data" as well as "Internet Protocol addresses" or "unique personal identifiers [or] online identifiers." Cal. Civ. Code § 1798.140. While Plaintiffs do not advance a claim under the CCPA, the legislature's definition in that statute illustrates that, at the very least, a reasonable juror could view the (s)WAA-off data Google collected via GA4F, including a user's unique device identifiers, as comprising a user's personal information.

B. Consent

Google argues that Plaintiffs consented to the collection of their pseudonymous data, but this too is unconvincing. The recently decided *Calhoun v. Google, LLC* is apposite. 113 F.4th 1141 (9th Cir. 2024). In that case, the class members challenged Google Chrome's sync function, averring that they believed choosing not to sync Chrome with their Google accounts would preclude the collection of their "personal information" by Google. *Id.* at *1143–44. While that case included an intrusion upon seclusion claim, the central inquiry on appeal was whether the plaintiffs consented to Google's conduct based on the viewpoint of a reasonable user encountering Google's disclosures (including the PP).

The Ninth Circuit confirmed that whether the plaintiffs consented turned on the terms of various disclosures and "whether a reasonable user reading them would think that he or she was consenting to the data collection, which collection Google has not disputed." *Id*. at 1148. The *Calhoun* court also distinguished *Hammerling v. Google, LLC*, No. 22-17024, 2024 WL 937247 at *3 (9th Cir. Mar. 5, 2024) (unpublished) and *Smith v. Facebook*, 745 Fed. App'x 8, 9 (9th Cir. 2018) (unpublished), cases where the "plaintiffs…had not argued that Facebook or Google had service-specific privacy policies that could reasonably be read to say the opposite of what its general privacy policies disclosed." *Calhoun*, 113 F.4th at 1149. "By contrast, and at least in the light most favorable to plaintiffs, Google did make a promise in its Chrome Privacy Policy that it would not collect certain information absent a user's voluntary decision to sync, so Google may be 'bound by [those] promises.'" *Id.* (quoting *Smith*, 745 Fed. App'x at 9). As in *Calhoun*, Google provides Plaintiffs with several disclosures, ranging from general privacy disclosures in its PP to more specific disclosures surrounding the WAA/(s)WAA buttons. From the perspective of a reasonable user, it is unclear Plaintiffs were consenting to the data collection at issue. With that background, analysis turns to the specific claims advanced by Plaintiffs in the FAC.

C. Invasion of privacy claims

While Plaintiffs' invasion of privacy claims, brought separately under the California constitution and common law, are distinct claims, they consist of substantially similar elements. The inquiry under either is whether "(1) there exists a reasonable expectation of privacy, and (2) [whether] the intrusion was highly offensive." *In re Facebook, Inc. Internet Tracking Litig.* ("*Facebook Tracking*"), 956 F.3d 589, 601 (9th Cir. 2020). Plaintiffs' common law tort claim also requires a showing of intent to commit the intrusion on Google's part.

1. Reasonable expectation of privacy

Google argues that Plaintiffs have no reasonable expectation of privacy in anonymized, aggregate data, invoking *Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1119 (9th Cir. 2020). In that case, however, the Ninth Circuit specifically declined to reach the issue: "We emphasize that this case also does not present the question whether standing could be based entirely on injury from

anonymized, aggregated uses of data." *Id*. at n.9. Indeed, "information need not be personally identifying to be private." *In re Google Referrer Header*, 465 F. Supp. 3d 999, 1009–10 (N.D. Cal. 2020); *see also Brown v. Google LLC*, 685 F.Supp.3d 909, 924 (2023) ("Plaintiffs have set forth specific facts demonstrating that the reason Google has access to their anonymous, aggregated data is through the collection and storage of information from users' private browsing history without consent."). Moreover, whether the data collected by Google constitutes personal information is not, as Google suggests, a foregone conclusion. *See In re Google RTB Consumer Priv. Litig.*, 606 F. Supp. 3d at 944.

Google invokes *Hammerling*, where the Ninth Circuit affirmed a district court's dismissal of these claims because Google's PP "expressly disclosed Google's intention to track [the plaintiffs'] activity on third-party apps. As a result, [they] have no reasonable expectation of privacy in that data." 2024 WL 937247 at *3. By contrast, Google's disclosures concerning the (s)WAA settings state that it governs a user's activity "on sites, apps, and devices that use Google services"—language almost identical as that in *Hammerling*— to describe data that Google will *not* save when (s)WAA is off. Following Google's logic, it is at least disputed here whether Plaintiffs have a reasonable expectation of privacy as to the (s)WAA-off data.

2. Highly offensive conduct

For Plaintiffs to succeed on their invasion of privacy claims, they need also show that the invasion of privacy was "highly offensive" to a reasonable person and unwarranted "so as to constitute an 'egregious breach of social norms.'" *Facebook Tracking*, 956 F.3d at 606 (quoting *Hernandez v. Hillsides, Inc.*, 47 Cal.4th 272, 295 (2009)). This inquiry "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." *Id.*

To emphasize the offensiveness of Google's conduct, Plaintiffs highlight the "vast and sensitive" nature of the information collected, *see Brown*, 685 F. Supp 3d at 941, as well as the significant profits Google makes resulting from its misconduct. Specifically, Plaintiffs suggest that Google can personalize ads based on (s)WAA-off data because Attribution/Conversion Tracking

is highly profitable for Google. In support, Plaintiff's technical expert, Jonathan Hochman, looks to the GA4F Help Center. There, Google indicates that a GA4F automatically collects certain "User Properties," including a user's IP address, age, gender, geolocation, "potentially even 'favorite food.'" Hochman Rep. 89, 99. Google also supposedly performs its (s)WAA "consent checks" only after it has collected and saved a myriad of unique and sensitive information from users, rendering the distinction between identifying and pseudonymous data (*i.e.*, GAIA and non-GAIA identifiers) meaningless. *Id*. at 86, 87.

This inquiry of Google's conduct turns on the nature of the information collected and whether a reasonable person would consider its collection to be an offensive intrusion. While Hochman's report indicates that Google creates these extensive and detailed marketing profiles of (s)WAA-off users which it then uses to gain high profits, those arguments are founded on a hypothetical scenario, rather than Google's actual conduct. Plaintiffs have provided no evidence that Google uses (s)WAA-off data to build highly targeted and invasive marketing profiles of (s)WAA-off users, only that Google has the technical capabilities of joining the identifiers it collects with more sensitive and personal data about the user. In fact, Google takes significant efforts to separate a (s)WAA-off users' GAIA-IDs from its device identifiers. Furthermore, "routine commercial behavior" is not a "highly offensive" invasion of privacy. *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012).

That Google can use this information to make money or improve its products or services is of little relevance. That principle applies *a fortiori* here as Google collects the (s)WAA-off data not simply to line its pockets, but for a free analytics tool intended to aid developers in understanding their apps and usage. Moreover, Plaintiffs have not explained how the (s)WAA-off data that Google collects constitute sensitive information that would offend a reasonable person and social norms. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) ("[T]he information allegedly disclosed to third parties included the unique device identifier number, personal data, and geolocation information from [p]laintiffs' iDevices. Even assuming this information was transmitted without Plaintiffs' knowledge and consent, a fact disputed by Defendants, such disclosure does not constitute an egregious breach of social norms.").

Ultimately, however, viewing the facts in the light most favorable to Plaintiffs, Google's conduct is at least arguably offensive because it collects (s)WAA-off data despite concerns raised by its employees and with the knowledge that its disclosures are ambiguous and deficient. In 2019, an employee who worked on Gmail shared internally that Google "would need to modify the [WAA disclosures] to indicate that WAA off is identical to being not logged into your account (data logged, but not tied to your account)." Later that year, he wrote again, highlighting that the WAA page indicates that WAA-off data should not be logged at all. Another employee wrote that "teams should not use user data at all if WAA is off," to align with what "most users expect." Several Google employees between 2017 and 2020 wrote that WAA was confusing and unclear to everyday users. *See* Plaintiffs' Opposition to Motion for Summary Judgment ("Plaintiffs' Opp.") at 12-13. Internal Google communications also indicate that Google knew it was being "intentionally vague" about the technical distinction between data collected within a Google account and that which is collected outside of it because the truth "could sound alarming to users."

Google argues that these comments are innocuous because they seek largely to identify potential technical improvements for Google services, and several of the employees making such remarks are unfamiliar with WAA. The concerns raised by Google employees are relevant, however, at the very least for tending to show that the WAA disclosures are subject to multiple interpretations. What is more, the remarks and Google's internal statements reflect a conscious decision to keep the WAA disclosures vague, which could suggest that Google acted in a highly offensive manner, thereby satisfying the intent element of the tort claim. Then again, these comments could also be ascribed to the unremarkable culture in large technology enterprises where employees simply offer improvements of the company's products or services. Whether Google or Plaintiffs' interpretation prevails is a triable issue of fact.

3. Harm

Google insists that Plaintiffs' invasion of privacy claims fail because Plaintiffs cannot establish that a "bare privacy harm" is actionable, as Article III injury alone cannot constitute harm to sustain the invasion of privacy claims (as well as CDAFA, discussed further below). In *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021), the Supreme Court held that, for purposes of

Article III standing, "only those plaintiffs who have been *concretely harmed* by a defendant's statutory violation may sue that private defendant over that violation in federal court." *Id.* at 427 (emphasis in original). The Court also noted that "[c]entral to assessing concreteness is whether the asserted harm has a 'close relationship to a harm traditionally recognized as providing a basis for lawsuits in American courts." *Id*. at 417 (internal quotations omitted); *Facebook Tracking*, 956 F.3d at 598 ("[V]iolations of the right to privacy have long been actionable at common law."). Additionally, as the Ninth Circuit indicated when discussing certain California privacy statutes, "under the privacy torts that form the backdrop for these modern statutes, the intrusion itself makes the defendant subject to liability . . . In other words, privacy torts do not always require additional consequences to be actionable." *Campbell*, 951 F.3d at 1117 (internal citations omitted).

Google insists that while Plaintiffs may have suffered Article III injury, they cannot show, class-wide, that they suffered harm under the invasion of privacy claims because the "emotional harms" associated with those claims are only available on an individual basis. Plaintiffs have offered no models or explanations for how these harms apply across the classes, and at the hearing, Plaintiffs' counsel admitted that if emotional harm was Plaintiffs' sole theory of harm, only nominal damages would be available to the class. Contrary to Google's view, however, that only nominal damages are available class-wide does not defeat Plaintiffs' invasion of privacy claims.

D. CDAFA

Plaintiffs aver, in their third claim, that Google's collection and use of (s)WAA-off data violates CDAFA, Cal. Penal Code § 502, *et seq*. CDAFA imposes liability on whoever "[k]nowingly accesses and without permission takes . . . any data from a computer." Cal. Penal Code § 502(c)(2). The statute allows an individual who "suffers damage or loss by reason of a violation" of the statute to bring a private civil action. Cal. Penal Code § 502(e)(1). Google seeks summary judgment for Plaintiffs' CDAFA claim on the grounds that it had permission to use (s)WAA-off data and that Plaintiffs suffered no damage or loss.

1. Permission[3]

CDAFA does not define "permission" within the text of the statute. Several cases in this district and the Ninth Circuit provide guidance as to the term's meaning for the purposes of CDAFA analysis, focusing on the plain meaning of the term and what the defendant knew while using the data. *See, e.g., In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1100 (N.D. Cal. 2015) ("'Permission' is defined as the 'act of permitting' or 'a license or liberty to do something; authorization.'") (quoting Black's Law Dictionary (8th ed. 2004)); *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1069 (9th Cir. 2016) (in concluding that the defendant violated CDAFA, holding that it "knew that it no longer had permission to access [the plaintiff's] computers at all"). Much of the authority on this issue comes from courts reviewing Computer Fraud and Abuse Act (CFAA) claims, 18 U.S.C. § 1030(a)(2). Courts in this district have held that CDAFA claims generally "rise or fall with . . . CFAA claims because the necessary elements of Section 502 do not differ materially from the necessary elements of the CFAA, except in terms of damages." *Meta Platforms, Inc. v. BrandTotal Ltd.*, 605 F. Supp. 3d 1218, 1260 (N.D. Cal. 2022) (citing *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 129 (N.D. Cal. 2020)). In the CFAA context, the Ninth Circuit defines "authorization" as "permission or power granted by an authority." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009).

First, Google argues that, as a matter of law, Plaintiffs explicitly consented because the default setting for (s)WAA gave Google permission to use their data, and toggling (s)WAA off did not revoke permission. Even if Plaintiffs impliedly granted Google permission to use their data *prior* to toggling (s)WAA off, this argument is lacking. *See Power Ventures*, 844 F.3d at 1069 (acknowledging that permission may be granted by implication in the context of CDAFA). What is relevant is whether toggling (s)WAA off *revoked* permission.[4] Google's generic disclosures in

[3] The parties interchangeably refer to this element under CDAFA as "permission" and "consent."

[4] If Google is correct that the WAA settings are of no import as to the data Google collected via GA4F, it is unclear how else a user may give Google consent to log that information to begin with (short of not signing up for a Google account), much less withdraw it.

the PP fail to show express or implied consent to the data use at issue because consent is only effective if directed "to the particular conduct, or to substantially the same conduct." *Tsao v. Desert Palace, Inc.*, 698 F.3d 1128, 1149 (9th Cir. 2012) (internal quotations omitted). Here, the permission prong of Plaintiffs' CDAFA claim turns on whether class members revoked permission when they toggled (s)WAA off.

When evaluating whether a party revoked permission in the context of CDAFA or CFAA, courts focus on the perspective of the defendant at the time they used the data. *See Power Ventures*, 844 F.3d at 1069. In *Power Ventures*, the Ninth Circuit held that a cease-and-desist letter sent by the plaintiff revoked any implied permission for the defendant to continue accessing their computers and using their data. The Ninth Circuit held that previously permitted use runs afoul of the CFAA (and therefore the CDAFA) "when such permission has been revoked explicitly." *Id*. at 1067. The Ninth Circuit did not hold that a cease-and-desist letter was required or articulate a specific test for revocation, instead focusing on what a defendant knew or should have known at the time of use. *Id.* at 1069 ("But when Facebook sent the cease-and-desist letter, Power, as it conceded, knew that it no longer had permission to access Facebook's computers at all . . . Power violated [the CDAFA].").

In this case, it is genuinely disputed whether Google knew or should have known that class members revoked permission to use (s)WAA-off data. Google contends that the description of the (s)WAA switch and what it controlled was plain and straightforward, clearly communicating that the access and use now at issue was beyond the scope of the setting. Plaintiffs disagree, arguing that they reasonably thought turning off (s)WAA meant that "Google would not collect or save their app activity." As explained above, evidence produced by Google during discovery, including deposition testimony by Google employees, indicates that the description of (s)WAA was ambiguous. Although Google disputes the applicability of that evidence, a reasonable juror could be convinced by either party's argument regarding the (s)WAA setting and Google's PP. Furthermore, Google has not explained how it received "consent" by (s)WAA-off users to collect the data if there was no meaningful way for users to provide that consent. Indeed, "consent is only

effective if the person alleging harm consented to the particular conduct, or to substantially the same conduct and if the alleged tortfeasor did not exceed the scope of that consent." *Brown*, 685 F. Supp. 3d at 926 (internal quotations omitted). Accordingly, it cannot be determined as a matter of law that Google had Plaintiffs' permission to use their data.

Google next argues that even if Plaintiffs did not give Google permission to use their (s)WAA-off data, the third-party app developers obtained consent from users as a condition of GA4F, so Google had permission to collect the data and its use did not violate CDAFA. Google says that it acted only as a "vendor" to those third-party apps and permission granted by users to a technology company extends to vendors who process such data. Even assuming Google acted as a vendor, no court has endorsed the position that when one technology company acts as a vendor for another, consent for the purposes of CDAFA analysis is coextensive with the party that obtained it. Google cites only to inapposite California Invasion of Privacy Act ("CIPA") cases in support of their position on this point. *See, e.g.*, *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823 (N.D. Cal. 2021). Unlike CFAA, CIPA has never been deemed substantially similar to CDAFA. Therefore, Google presents no relevant authority to show that under CDAFA, permission given by third parties to use (s)WAA-off data satisfies the statute's permission requirement.

Google's third-party permission argument is not only unsupported by any applicable caselaw but also in tension with relevant Ninth Circuit precedent. In *United States v. Nosal*, the Ninth Circuit held that "once authorization to access a computer has been affirmatively revoked, [a defendant] cannot sidestep the statute by going through the back door and accessing the computer through a third party. Unequivocal revocation of computer access closes both the front door and the back door." 844 F.3d 1024, 1028 (9th Cir. 2016) (discussing the authorization prong of the CFAA). Assuming, then, that Plaintiffs did revoke permission when they toggled (s)WAA off, whether a third party granted permission is irrelevant. Instead, what matters is whether Google knew or should have known that Plaintiffs revoked permission to use their data, a material fact that is genuinely disputed.

Google also contends that if a plaintiff was indeed confused about the limitations of the

WAA or (s)WAA settings, that confusion would undermine Plaintiffs' class-wide claims because it otherwise received clear consent for pseudonymous record-keeping. As explained, whether Google received consent for its conduct is not a sure-fire proposition. More critically, Google confuses the issue here: viewing the facts in the light most favorable to Plaintiffs, it is a disputed fact, not an individualized inquiry, whether the class members' uniform conduct of turning (s)WAA off withdrew their consent for Google to "save app activity data." This identical conduct, as explained in the class certification order, still warrants class treatment. Moreover, Google's disclosures were uniform to all class members and its treatment of the classes' data was also identical. Its own imprecision does not undermine predominance.

2. Damage or Loss

CDAFA neither defines nor sets a monetary threshold for "damage or loss." *Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461, 487 (N.D. Cal. 2021). Rather, "under the plain language of the statute, any amount of damage or loss may be sufficient." *Facebook, Inc. v. Power Ventures, Inc.*, No. 08-cv-05780-JW, 2010 WL 3291750, at *4 (N.D. Cal. July 20, 2010). Plaintiffs argue that at least five injuries establish "damage or loss" under CDAFA.

a. Deprivation of privacy

This damage theory rests entirely on the viability of Plaintiffs' other two claims and requires a showing of harm. As discussed above, Plaintiffs are unable to show that they are entitled to more than nominal damages resulting from the emotional harms associated with their deprivation of privacy. They offer no concrete models or theories that this harm constitutes more than simply an emotional injury. However, Plaintiffs have other damage or loss theories that provide a basis to satisfy this element of CDAFA.

b. Disgorgement of profits

Plaintiffs argue that they experienced damage or loss because Google illegally profited from the use of their data. Plaintiffs rely on *Facebook Tracking*, where the Ninth Circuit held that "California law recognizes a right to disgorgement of profits resulting from unjust enrichment, even where an individual has not suffered a corresponding loss." 956 F.3d at 599. Google

responds that, in light of *TransUnion*, Plaintiff's disgorgement of profits theory of damage or loss is untenable under CDAFA. 594 U.S at 417.

Plaintiffs' disgorgement theory is compatible with *TransUnion*, which held that, when determining which injuries are sufficiently concrete, "history and tradition offer a meaningful guide." *Id.* at 424 (citation omitted). Certain harms "readily qualify as concrete injuries under Article III. The most obvious are traditional tangible harms, such as physical harms and monetary harms." *Id.* at 425. Intangible harms, such as "disclosure of private information" or "intrusion upon seclusion", have also been traditionally recognized. *Id.* Google argues that its "harmless data collection" does not serve as a basis to disgorge its profits because it does not constitute a concrete injury.

Notwithstanding that it is disputed whether Google's data collection was "harmless," *Brown v. Google LLC* is instructive in showing why Plaintiffs' intangible harms are sufficiently concrete to constitute damage or loss under current law. 685 F. Supp. 3d 909 (N.D. Cal. 2023). In that case, decided after *TransUnion*, the court held that the plaintiffs satisfied CDAFA's damage or loss requirement because they had "a stake in the value of their misappropriated data." *Id.* at 940. Relying on *Facebook Tracking*, the court held that the plaintiffs could state an economic injury for their misappropriated data. *Id.*; *Facebook Tracking*, 956 F.3d 589 at 600. The court also denied summary judgment as to the defendant's argument that plaintiffs lacked standing to seek an unjust enrichment remedy, holding that *Facebook Tracking* was still good law. *Brown*, 685 F. Supp. 3d at 926. Here, Plaintiffs have a stake in the value of their data. As in *Brown*, where the court denied summary judgment on the issue of damage or loss "because plaintiffs proffer[ed] evidence that there [was] a market for their data," Plaintiffs here similarly present evidence that their data has economic value. 685 F. Supp. 3d at 940. Accordingly, a reasonable juror could find that Plaintiffs suffered damage or loss because Google profited from the misappropriation of their data.

c. Failure to pay for collected data

Third, Plaintiffs argue that they suffered damage or loss because Google failed to pay for

the data it collected despite there being a market for it. This theory of damage or loss is closely related to Plaintiffs second theory. *See Brown*, 685 F. Supp. 3d at 925-26, 940 (discussing unjust enrichment and economic injury for misappropriated data). Plaintiffs argue that they suffered damage or loss because Google took something of economic value from them without their permission. Google insists that this theory fails because Plaintiffs did not wish to sell their data and, even if they did, their data did not diminish in value because of its conduct. However, "under California law, [a] stake in unjustly earned profits exists regardless of whether an individual planned to sell his or her data or whether the individual's data is made less valuable." *Facebook Tracking*, 956 F.3d at 600. It remains disputed whether Plaintiffs suffered damage or loss because Google failed to pay for their data despite the existence of a market.

d. Depletion of battery and bandwidth

Fourth, Plaintiffs proffer evidence that Google's unauthorized access depleted their devices' battery and bandwidth, causing damage or loss. Courts recognize depletion of battery and computing resources as acceptable forms of damage or loss for the purposes of a CDAFA claim. *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1065 (N.D. Cal. 2015); *Williams v. Facebook, Inc.*, 498 F. Supp. 3d 1189, 1199 (N.D. Cal. 2019). While Plaintiffs have provided no evidence about how much device battery life and bandwidth was depleted, they point to internal Google documents that suggest Google Analytics impacts battery-life of a device. Google points out that Plaintiffs failed to present a damage model at class certification based on this harm, and Plaintiffs concede that only nominal damages would be available to them under this theory of liability. As the statute sets no minimum threshold for damage or loss, even small harms due to depletion of battery and bandwidth satisfy CDAFA's requirements. At this stage, Plaintiffs have provided sufficient evidence to show harm for at least nominal damages under this theory.

e. Denial of benefit of the bargain

Finally, Plaintiffs argue that they suffered damage or loss because class members did not receive the "benefit of their bargain" with Google, a concept linked to their now dismissed breach of contract claim. Dkt. 127, 209. Plaintiffs have offered no authority that denial of the benefit of

the bargain constitutes damage for CDAFA absent a contract claim.

E. Motions to Seal

The parties have filed administrative motions to seal portions of their briefing. Plaintiffs move to seal highlighted portions of Exhibit 4 of its Opposition on the grounds that it contains personally identifiable information, which is deemed private pursuant to the Protective Order.

Google has moved to seal no portion of the Opposition or its Reply brief (and its Motion for Summary Judgment was filed publicly). Instead, Google seeks only to seal portions of 16 exhibits submitted alongside the Opposition and Reply briefs and 6 exhibits in full. Google subsequently withdrew its request to seal one sentence from Exhibit 34. Google raises several grounds as the basis for its motion to seal: first, it seeks to seal commercially sensitive information, including its internal research methodologies and forward-looking strategies and deliberations. It also seeks to seal private documents regarding the technical details of Google's internal systems, references to internal code names, and non-public email addresses.

The parties' motions to seal have satisfied the "compelling reasons" standard for dispositive motions. *See Ctr. for Auto Safety v. Chrysler Grp.*, 809 F.3d 1092, 1098–1099 (9th Cir. 2016). The sealing questions are tailored narrowly in order to avoid impacting the public's understanding of this case. Accordingly, the motions to seal are granted.

V. CONCLUSION

For the reasons explained above, Google's motion for summary judgment is denied and the pending motions to seal are granted. The parties shall file public versions of their briefs and related exhibits in accordance with the sealing order within one week of the date of this order.

IT IS SO ORDERED.

Dated: January 7, 2025

RICHARD SEEBORG

Chief United States District Judge