UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JOHN DOE I, et al.,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No. 23-cv-02431-VC

ORDER GRANTING MOTION TO DISMISS

Re: Dkt. No. 88

This is another pixel case. In many pixel cases, the plaintiffs sue the owner of the web property they interacted with, alleging that the owner installed source code that caused their personal information to be transmitted to a third party. But in this case, the plaintiffs have sued the third party that offers the source code: Google. They allege that their health care providers use Google source code to analyze traffic on their web properties, that their personal health information is transmitted to Google as part of this process, and that Google feeds this information into its own advertising machinery. For this, the plaintiffs assert, Google is liable for violating their privacy rights.

There are several related problems with the complaint. First, by the plaintiffs' own allegations, Google has admonished health care providers not to use the source code in a way that causes users' personal health information to be transmitted to Google. Second, the allegations in the complaint are too vague to support an inference that the providers have, contrary to this admonition, caused Google to receive the plaintiffs' personal health information. And third, to the extent the complaint could be read to support an inference that health care providers may sometimes use Google products in a way that causes Google to receive personal

health information, the complaint does not adequately allege that Google intends to receive this information, or that Google intends to feed the information into its own advertising machinery.

Primarily for these reasons, the complaint is dismissed in its entirety. The Court is increasingly skeptical, based on what's transpired in this case so far, that the plaintiffs can successfully amend their complaint. But in an abundance of caution, they will get one more chance to do so.

I.

The plaintiffs are twelve people proceeding anonymously who allege that Google unlawfully tracks, collects, and monetizes their private health information through source code that is "secretly embedded" on their health care providers' websites. Dkt. No. 86 at ¶ 5. According to the plaintiffs, Google's actions violate federal and state law, and contradict Google's own policies about how it collects and uses data. The plaintiffs bring this action on behalf of a proposed class of both Google account holders and non-Google account holders. The health care providers themselves are not named as defendants, although the attorneys who brought this case have also filed a lawsuit against one of the providers in a separate case. *See Kurowski v. Rush System for Health*, 683 F. Supp. 3d 836 (N.D. Ill. 2023).

The source code at issue is associated with several different Google products, including Google Analytics, Google Ads, and Google Display Ads.[1] Google offers the source code for these products "in a copy-and-paste format" for website developers to deploy to analyze users' activities online and to market their companies. Google Analytics is a tool that allows website and app developers to understand how users engage with a given website or app. Google

[1] The plaintiffs attach 55 exhibits to their complaint, most of which are resources Google makes publicly available that explain how their various products operate. The Court can consider these documents on a motion to dismiss as they are expressly incorporated into the complaint. Google also asks the Court to take judicial notice of 21 additional exhibits. The plaintiffs do not oppose taking judicial notice of Google's exhibits 1-5, as they are documents published by Google similar to those incorporated into the complaint. However, the plaintiffs object to judicially noticing exhibits 6-21, as they are privacy policies and terms of service for the non-party health care providers. These exhibits are not incorporated by reference into the complaint, nor are they judicially noticeable as their accuracy can reasonably be questioned. *See* Fed. R. Evid. 201(b)(2).

Analytics collects standard information when a user interacts with a webpage, such as browser, network, and location information, or events like a user's clicks or searches. Google Analytics also uses cookies, which are "small text files that are saved to web browsers" to collect data about web usage. Google Ads is a separate product associated with Google's search engine that allows a business to "create online ads to reach people exactly when they're interested in the products and services that" are offered by that business. Google Ads also uses cookies to collect data about users as they interact with Google and non-Google web properties. Google Display Ads is a third product that offers advertising space on a network of partner sites and apps. Like the other products, Display Ads uses cookies to collect data. Although each product has its own source code and specific cookies associated with it, the plaintiffs refer to all these products generically as Google source code.[2]

According to the complaint, Google source code is present on 91 percent of the roughly 5,000 health care provider web properties they investigated. The plaintiffs allege that the presence of Google source code on health care provider web properties results in two general buckets of wrongdoing. First, the source code allegedly *intercepts* private health information by redirecting the plaintiffs' interactions on their providers' web properties to Google's servers. Second, Google allegedly *uses* the private health information sent to it in its own advertising systems to make money.

After this lawsuit was filed, it was consolidated with another similar action, and the plaintiffs filed a new consolidated class action complaint. The plaintiffs then moved for a preliminary injunction. The Court denied the motion, in part because of the plaintiffs' failure to show that Google was unlawfully using the plaintiffs' private health information. The plaintiffs then filed yet another version of the complaint. Google has once again moved to dismiss.

[2] The plaintiffs also include allegations about five other Google products—Google Tag, Google Tag Manager, Google Firebase SDK, Google APIs, and YouTube—but the plaintiffs allege that the products described above are the "three primary Google products and services which leverage Google Source Code."

II.

The complaint is 188 pages long and contains twelve claims against Google. The next section addresses each separate claim. This section discusses three overarching problems with the complaint that affect the outcome for most of the claims.

A.

The complaint makes repeated reference to an "investigation" performed by plaintiffs' counsel and their experts. Specifically, the plaintiffs allege they examined 5,297 health care provider "web properties," and determined Google source code is present on 91 percent of these properties. *See* Dkt. No. 86 at ¶ 155. The plaintiffs also allege that "investigation reveals that Google intercepted" information about each plaintiff's specific medical needs and conditions based on each plaintiff's interactions with their provider's websites. *See id.* at ¶¶ 20-31.

But the plaintiffs provide no details about their investigation, nor do they explain how they have determined that their private health information has been intercepted by Google. Instead, the plaintiffs appear to assume that because there is Google source code somewhere on the health care providers' web properties, that automatically results in Google intercepting any interaction the plaintiffs have had with that website. They say as much about one specific health care entity when they allege that, "because the Google Source Code appears on the MedStar website," Google's tracking of patients "occurs the moment that patients begin interacting with their Health Care Provider (e.g. MedStar), and it continues for almost every interaction and communication that occurs thereafter, including when a patient interacts with 'authenticated' web pages, like the MedStar patient portal." *Id.* at ¶ 58. The documents incorporated by reference into the complaint do not support this assumption; indeed, they appear to contradict it.

According to these documents, Google tells "HIPAA-regulated entities," like the health care providers here, to "only use Google Analytics on pages that are not HIPAA-covered" and to "identify pages" on their websites "that do not relate to the provision of health care services." *Id.* at ¶ 303. Google also directs health care providers to the Department of Health and Human Services bulletin that offers guidance on how HIPAA covered entities should use tracking

technology.[3] *Id.* Consistent with Google's own directions, the HHS guidance warns health care entities that using tracking technology on certain webpages, such as user-authenticated pages, will likely result in the transmission of protected health information. At the same time, HHS clarifies that tracking technology on many unauthenticated pages will not lead to protected health information being revealed. *See* Dkt. No. 86-37 at 5-6. These documents make clear that what matters is where on the web property the source code exists. The presence of source code on a homepage for a provider's website will result in different information being transmitted than the presence of source code on an appointment scheduling page within a patient portal. Based on both Google's instructions and HHS's guidance, the source code can exist on one page of a website but not another. Therefore, the plaintiffs cannot simply allege that a "web property" contains source code and then assume this means every single page on that property contains source code.

This problem is compounded by the plaintiffs' failure to use precise language when describing the type of information that is allegedly transmitted. Going back to the MedStar example, the plaintiffs repeatedly allege that data sent to Google "may include" specific information like patient device identifiers or search terms. *See* Dkt. No. 86 at ¶¶ 60-64. When making allegations about Google Ads and Google Display Ads, the plaintiffs are equally abstract. They say that "when the Google source code for Google Ads is present on a health care provider's web property," various information gets redirected to Google. *See id.* at ¶¶ 76-81 (Google Ads), 88-92 (Google Display Ads). The use of this type of indefinite language makes it unclear what are true factual allegations and what is just speculation.

In short, the allegation that 91% of health provider "web properties" contain Google source code seems powerful in the abstract, but it becomes largely meaningless (to the point of seeming intentionally slippery) once you sift through the fine print of the plaintiffs' 188-page

[3] HHS defines "tracking technology" as "a script or code on a website or mobile app used to gather information about users or their actions as they interact with a website or mobile app." Dkt. No. 86-37 at 4. This definition encompasses the Google products at issue in this suit.

complaint and accompanying 55 exhibits. Those documents leave the reader conspicuously unable to discern whether the source code is placed on web pages where it doesn't belong, and if so, how commonly this happens.

B.

The complaint also relies heavily on Google's own product descriptions to allege that Google is obtaining personal health information from its health care provider clients. The problem is that these product descriptions are generic—they describe various ways in which Google's products are capable of operating generally, not how they operate when particular health care providers use them. Thus, the complaint adequately alleges that providers *could* configure and use the products in a way that would cause personal health information to be transmitted to Google. But instead of offering factual allegations about how the plaintiffs' various providers are *actually* using Google's products, the plaintiffs allege hypothetical examples—based on the generic product descriptions—of how various product features could be used in ways that could result in privacy violations. As just one example, the complaint describes how a hypothetical pharmaceutical company could target ads to patients who have shared communications about the company's drugs. Accordingly, the plaintiffs allege that "a patient who searched for a diabetes medication may start seeing advertisements for diabetes medications across their different devices." *See id.* ¶ 144-45. But there are no allegations that the plaintiffs in this case ever saw advertisements for prescription medications after interacting with their health care provider's website. In fact, there are no allegations that any plaintiff here ever saw any targeted advertisements related to their health at all.

In sum, the plaintiffs are not merely assuming that Google source code is being placed on particular web pages. They are also assuming that particular features of Google's products are being enabled on those pages, based simply on the fact that those features happen to be described in Google's generic product descriptions.

C.

Finally, most of the legal claims asserted by the plaintiffs require an allegation that Google actually intended to acquire or use people's personal health information. The plaintiffs are all over the map on the issue of intent, and ultimately they fail to offer a coherent narrative.

As a threshold matter, the plaintiffs set the legal bar too low when describing the intent requirement for their claims. They appear to argue that intent only requires awareness that information is likely being transmitted. *See* Dkt. No. 97 at 18. On this theory, perhaps the complaint would adequately allege intent—no matter how often Google tells its health care provider clients not to attach source code to web pages that could glean private health information, Google must know that providers will sometimes make mistakes. But this is not the right way to think about intent.

The plaintiffs cite two cases—both discussing intent in the context of the Federal Wiretap Act. The first, *In re Google Assistant Privacy Litigation*, does contain language suggesting that awareness alone could be sufficient. 457 F. Supp. 3d 797, 815 (N.D. Cal. 2020). But the second case, which is binding, undermines the plaintiffs' position. It explains that the word intentionally, as used in the federal wiretapping statute, means "purposefully and deliberately and not as a result of accident or mistake." *United States v. Christensen*, 828 F.3d 763, 790 (9th Cir. 2015). This suggests something more than mere awareness that an interception might occur due to the failure of the health providers to follow instructions. Rather, "the operative question under § 2511 is whether the defendant acted consciously and deliberately with the goal of intercepting wire communications." *Id.* at 791. This is not merely true with respect to the Wiretap Act claim; the plaintiffs have offered no authority to suggest that the intent requirement is less stringent for the other claims in their lawsuit that include an intent requirement.

With this understanding, the plaintiffs have not adequately alleged that Google intentionally obtained patients' private health information. As already discussed, the complaint acknowledges that Google repeatedly told developers not to send personally identifiable information through use of its source code. *See id.* at ¶¶ 331-37. And for health care providers

specifically, Google warned that they must not use its source code in ways that would result in HIPAA-covered information being sent to Google. The takeaway from these allegations is that Google purposefully acted so as *not* to receive any personal health information.

Relatedly, the plaintiffs try to allege that Google is capable of preventing the inadvertent transmission of private information from health care provider websites, and that its failure to do so is reflective of an intent to obtain the information. But these allegations are, once again, quite vague. It's not clear from the allegations that Google can actually prevent private health information from being sent to it, at least short of preventing health care providers from using its source code altogether. The plaintiffs allege that Google "can readily identify the web properties" that use its source code. *Id.* at ¶ 205. They also allege that Google has tools to identify which web properties belong to health care providers. *Id.* at ¶ 206. As a result, the plaintiffs allege, "if Google wished to do so, it could stop collecting the illicit health information." *Id.* at ¶ 224. But assuming all that is true, it seems like the only way Google could prevent the collection of health information from health care providers would be to completely restrict them from using its source code. From a policy perspective, that is certainly one path forward. However, HHS does not prohibit the use of "tracking technologies" on health care provider websites. Instead, as previously detailed, HHS simply cautions providers to be careful how they use such technology so as not to inadvertently disclose private health information. There is nothing inherently unlawful about Google offering its source code to health care providers, and no inference can be drawn that Google's failure to prevent providers from using its source code entirely somehow reveals an intent to receive private health information—at least not against the backdrop of Google's admonitions that providers must avoid transmitting it.

Confronted with the possibility that their own allegations negate intent, the plaintiffs pivot to saying that Google's admonitions to health care providers are of no import because they are simply self-serving claims. According to the plaintiffs, because Google did not "prevent the foreseeable transmission of protected information," Google's admonitions "do no more than provide a modicum of deniability for Google." Dkt. No. 97 at 18-19. But the plaintiffs offer no

support for their assertions that Google's instructions are just a ruse to mask the company's true objective. Even when invited to address this Court's concerns with these exact arguments—and to do so using relevant quotes from the complaint—the plaintiffs just repeat the same conclusory arguments. *See* Dkt. No. 146 at 6-7.

It's possible that this ruling is contrary to Judge Orrick's analysis of intent in a similar pixel case against Meta. *See Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1076 (N.D. Cal. 2023). Like Google, Meta argued that the plaintiffs failed to allege intent because it was the health care providers who installed Meta Pixel, and because Meta also warned developers not to send it sensitive information. Judge Orrick rejected Meta's arguments and concluded that intent was adequately alleged. *Id*. ("While plaintiffs acknowledge that Meta may tell third parties and Facebook users that it intends to prevent receipt of sensitive health information, plaintiffs contend that is not what Meta *really* intends. . . . What Meta's true intent is, what steps it actually took to prevent receipt of health information, the efficacy of filtering tools, and the technological feasibility of implementing other measures to prevent the transfer of health information, all turn on disputed questions of fact that need development on a full evidentiary record. . . . At this stage, intent has been adequately alleged."). It's possible that the difference between Judge Orrick's ruling and this one lies in what precisely was alleged in each complaint. But to the extent Judge Orrick's ruling stands for the notion that allegations like the ones in this case are sufficient to plead intent, this Court disagrees. If a plaintiff alleges that the clients of a source code provider use the code contrary to the provider's instructions, the plaintiff should not be able to get around the intent requirement by simply intoning that the source code provider intended for the clients not to follow instructions.

Indeed, by insisting that Google's admonitions to health care providers are part of a plot to steal private health information from its clients, the plaintiffs may well be subjecting their intent-related allegations to the heightened pleading standard of Federal Rule of Civil Procedure 9(b). *See Rodriguez v. Google LLC*, No. 20-CV-04688-RS, 2021 WL 2026726, at *3 (N.D. Cal. May 21, 2021); *but see Smith v. Google, LLC*, No. 23-CV-03527-PCP, 2024 WL 2808270, at *5

(N.D. Cal. June 3, 2024). But given the allegations stemming from the complaint and the documents incorporated by reference, the plaintiffs do not even satisfy the basic Rule 8 standard.

III.

It mostly follows from the preceding section that all twelve claims must be dismissed.

Electronic Communications Privacy Act. The Federal Wiretap Act makes it unlawful to intentionally intercept an electronic communication. *See* 18 U.S.C. § 2511(1). To state a claim, the plaintiffs must plausibly allege Google (1) intentionally (2) intercepted (3) the contents of (4) plaintiffs' electronic communications (5) using a device. *See In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003). There is an exception to liability for a person who is a party to the communication or "where one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(d). This exception applies unless the interception occurred "for the purpose of committing any criminal or tortious act." *Id.*

The plaintiffs have failed to adequately allege a violation of the Wiretap Act because, as discussed earlier, they have failed to allege Google intentionally intercepted their personal health information. Additionally, the plaintiffs have included allegations that seem to establish the one-party consent defense. The alleged interception of private health information only occurs because the health care providers choose to install Google source code on their web properties. This must mean the providers consented to the operation of Google source code.

To get around the one-party consent problem, the plaintiffs assert that any consent was improperly obtained because Google gave health care providers false impressions about how its source code operated. *See* Dkt. No. 86 at ¶¶ 332-36. The plaintiffs suggest that it was Google's false promises about whether information sent to it would be pseudonymous or anonymous that induced the providers to utilize Google source code. At the hearing, the plaintiffs confirmed this was their argument, asserting that consent was obtained "under false pretenses."

The problem is that, like the intent allegations discussed above, these seem like fraud-based allegations. *See Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1105 (9th Cir. 2003). In cases "where fraud is not an essential element of a claim," any "allegations ('averments') of

fraudulent conduct must satisfy the heightened pleading requirements of Rule 9(b)." *Id*. The plaintiffs respond by intoning that the issue of whether a party to the communication consented to interception by a third party relates only to an affirmative defense and is not an element of a Wiretap Act claim. Normally, that might be a good response, because generally a plaintiff need not plead the absence of an affirmative defense at all, and so generally it would be inappropriate to say that a heightened pleading standard applies to allegations about an affirmative defense. But here, absent allegations of fraud, the consent defense to Wiretap Act liability would leap off the page. The Court would have no choice but to rule that the plaintiffs pled themselves out of a Wiretap Act claim by including allegations showing that health care providers "consented" by placing the source code on their web properties for the purpose of utilizing Google's services. So the plaintiffs have included fraud-based allegations to avoid dismissal of this claim based on consent. Under these circumstances, it seems appropriate to apply a Rule 9(b) pleading standard to these fraud-based allegations. But again, the allegations of Google's deception are so vague that they fail even under Rule 8.[4]

California Invasion of Privacy Act. To state a claim under this statute, the plaintiffs must show that (1) by means of a machine, instrument, or contrivance, Google (2) willfully and without the consent of all parties (3) read, attempted to read, or to learn the contents or meaning of any communication, (4) while the communication was in transit (5) to or from any place in California. *See* Cal. Penal Code § 631(a). California also imposes liability on a person who,

[4] Apart from the allegations about false impressions, the plaintiffs also argue that the one-party consent exception cannot apply because Google intercepted the plaintiffs' health information for the purpose of committing a criminal or tortious act. *See* 18 U.S.C. § 2511(2)(d). But for this exception to the exception to apply, the "criminal or tortious purpose must be separate and independent from the act of the recording." *Planned Parenthood Federation of America, Inc. v. Newman*, 51 F.4th 1125, 1136 (9th Cir. 2022). It is not about whether the interception violated another law but "whether the *purpose* for the interception—its intended use—was criminal or tortious." *Id.* (quoting *Sussman v. American Broadcast Companies, Inc.*, 186 F.3d 1200, 1202 (9th Cir. 1999)). And as other courts have observed, Google's purpose in offering these products "has plainly not been to perpetuate torts on millions of Internet users, but to make money." *Rodriguez v. Google LLC*, 2021 WL 2026726, *6 n.8 (N.D. Cal. May 21, 2021) (quoting *In re Google Inc. Gmail Litigation*, No. 13-MD-02430-LHK, 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014)).

"intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication." Cal. Penal Code § 632(a). Although these are both criminal statutes, section 637.2 gives anyone "injured by a violation of this chapter" a civil cause of action.

Google raises two primary arguments against the plaintiffs' CIPA claims. First, Google contends that it did not read, attempt to read, or learn the contents of any communication. Google asserts that it merely offers a tool for websites to record user interactions for themselves. This, as Google sees it, is akin to providing a tape recorder for a party to use during a communication. *See Rogers v. Ulrich*, 52 Cal. App. 3d 894, 899 (1975) (holding that the use of a tape recorder by a party to the communication did not violate CIPA). And because Google is simply giving websites a service that allows them to record and analyze their own data, Google contends it is not itself engaging in the conduct—reading or learning the contents of communications—prohibited by the statute. *See Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 833 (N.D. Cal. 2021); *Williams v. What If Holdings, LLC*, No. 22-CV-03780-WHA, 2022 WL 17869275, at *3 (N.D. Cal. Dec. 22, 2022).

The plaintiffs respond that Google is not acting as a passive provider of a tape-recording service. Rather, they assert that Google is reading and learning the contents of the communications itself because it is aggregating and using the data it receives to feed its own advertising machine. The plaintiffs allege that Google compiles "detailed reports on all activity that occurs on a web-property" and that Google can monetize the data it collects through its ad business. *See* Dkt. No. 86 at ¶¶ 123-30. Thus, according to the plaintiffs, Google is reading and learning the contents of the communications transmitted via its source code.

The allegation that Google creates reports of user activity on a given web property does seem to support an inference that Google is doing more than simply acting as a tape recorder. But the complaint runs into two problems. First, any reports Google creates would only capture activity on pages where Google source code is present and, as described earlier, the plaintiffs do not adequately allege where on a web property the source code actually exists. This means it's

not clear whether Google is, in fact, reading and learning the contents of the plaintiffs' private health information. Second, there is again the issue of intent. As already detailed, the complaint and incorporated materials stand for the proposition that Google does not want to receive private health information and has instructed providers not to send it. CIPA liability only extends to willful or intentional conduct, so even if some private health information is inadvertently sent to Google—and subsequently gets integrated into the reports—the plaintiffs fail to plausibly allege Google is intentionally reading or learning the contents of the plaintiffs' private health communications.

Common law/Constitutional Privacy. The plaintiffs bring separate claims for invasion of privacy under the California Constitution and the common law. Given the overlap in these claims, courts consider them together and "ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *See In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 601 (9th Cir. 2020). The inquiry about the offensiveness of an intrusion involves examining "all of the surrounding circumstances, including the degree and setting of the intrusion and the intruder's motives and objectives." *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 295 (2009). "The California Constitution and the common law set a high bar for an invasion of privacy claim." *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012).

Given the two flawed assumptions the plaintiffs make—about where Google source code is present on a given web property and about what features of Google's products the health care providers have enabled—there is no way to understand the nature of the intrusion, and thus no way to assess whether it rises to the level of being highly offensive. Moreover, as already discussed, the plaintiffs have not adequately alleged intent, which is a necessary element of an invasion of privacy claim. *See In re iPhone Application Litigation*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) ("Even negligent conduct that leads to theft of highly personal information, including social security numbers, does not 'approach [the] standard' of actionable conduct under the California Constitution.").

Unfair Competition Law. To bring a claim under California's Unfair Competition Law, a plaintiff must have statutory standing, which requires the plaintiff to have suffered an injury in fact and lost money or property because of the unfair competition. *See Birdsong v. Apple, Inc.*, 590 F.3d 955, 959 (9th Cir. 2009). The plaintiffs argue that they satisfy the UCL standing requirements because they have alleged that their health information is property under California law and that they have lost money because it has economic value.

On the issue of personal information as property under California law, the plaintiffs rely on two cases. The first, *People v. Kwok*, is a criminal case from a California Court of Appeal about whether making an unauthorized copy of a key to a residence constitutes theft. 63 Cal. App. 4th 1236 (1998). The court analogized "making an unauthorized copy of a borrowed key" to "making an unauthorized copy of a trade secret or an unauthorized copy of computer data," concluding that all three are examples of theft. *Id.* at 1251. But the circumstances addressed in *Kwok*—whether the copying of a tangible object is theft—does little to answer the question of whether California law considers personal information, like the information at issue in this case, to be property. The second case, *Calhoun v. Google LLC*, does say "that users have a property interest in their personal information." 526 F. Supp. 3d 605, 635 (N.D. Cal. 2021). But the support cited for this proposition is also tenuous. The first case is a different California Court of Appeal opinion that deals with whether an identity theft victim could recover the surplus funds of a foreclosed property that was purchased using the victim's stolen personal information. *See CTC Real Estate Services v. Lepe*, 140 Cal. App. 4th 856, 860 (2006). The second case is a Ninth Circuit opinion that determined only that the plaintiffs had an entitlement to the profits earned off personal data for purposes of Article III standing. *See In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 600 (9th Cir. 2020). Neither case relied on by *Calhoun* makes it clear that there is a property interest in personal information. *Compare In re iPhone Application Litigation*, 844 F. Supp. 2d 1040, 1075 (N.D. Cal. 2012) ("The weight of authority holds that a plaintiff's personal information does not constitute property."); *see also McClung v. AddShopper, Inc.*, No. 23-CV-01996-VC, 2024 WL 189006, at *2 & n.2 (N.D. Cal. Jan. 17, 2024) (discussing

the limits of the *Facebook Internet Tracking* decision).

The loss of personal data is also not sufficient to demonstrate an economic injury. To be sure, there are cases that support the plaintiffs' position. *See, e.g.*, *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 636 (N.D. Cal. 2021) ("Plaintiffs who suffered a loss of their personal information suffered economic injury and had standing."). But this Court agrees with Judge Breyer that simply because a plaintiff's information "is valuable in the abstract," and simply because a company "might have made money from it," that does not mean that the plaintiff has "lost money or property as a result." *Hazel v. Prudential Fin., Inc.*, No. 22-CV-07465-CRB, 2023 WL 3933073, at *6 (N.D. Cal. June 9, 2023). *See also McClung*, 2024 WL 189006, at *2; *Katz-Lacabe v. Oracle America, Inc.*, 668 F. Supp. 3d 928, 943 (N.D. Cal. 2023). This is true even when, as here, there are allegations that the plaintiffs' personal data has a measurable monetary value and there is a market for such data that the plaintiffs could easily access. Such allegations fail to explain why any alleged acquisition of personal information would necessarily mean that the plaintiffs could not still sell their data in the market they allege exists.

Trespass to Chattels. Trespass to chattels has been coined "the little brother of conversion" as it "allows recovery for interferences with possession of personal property not sufficiently important to be classed as conversion." *Best Carpet Values, Inc. v. Google, LLC*, 90 F.4th 962, 967 (9th Cir. 2024). Under California law, a trespass to chattels claim exists "where an intentional interference with the *possession* of personal property causes injury." *Id.* at 968 (quoting *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1350-51 (2003)).

The plaintiffs allege that Google is liable for this tort based on the alleged intrusion of Google source code onto the plaintiffs' computing devices when they visit their health care providers' websites. According to the complaint, "Google designed its source code for the purpose of lodging Google Cookies on computing devices." Dkt. No. 86 ¶ 482-83. Because the plaintiffs' allegations of injury are entirely conclusory, they have failed to state a claim for trespass to chattels.

Under California law, "decisions finding electronic contact to be a trespass to computer

systems have generally involved some actual or threatened interference with the computers' functioning." *Hamidi*, 30 Cal. 4th at 1353. Here, the plaintiffs allege that the placement of cookies on their devices "reduces storage, disk space, and performance" but they offer no factual support for these allegations. *See* Dkt. No. 86 at ¶ 488. And it is not obvious how the presence on one's computer of the cookies from the providers' websites would result in any cognizable reduction in storage, disk space, or performance.

The plaintiffs also allege that the presence of Google source code renders their devices useless for exchanging private communications with their health care providers. *See id.* at ¶ 491. But nothing about the source code or the existence of cookies physically impairs the functioning of the plaintiffs' computing devices. And the decision not to use one's computer to communicate with a specific entity is not the same as actually being deprived of the ability to use one's computer.

Conversion. To establish the tort of conversion, "a plaintiff must show ownership or right to possession of property, wrongful disposition of the property right and damages." *Kremen v. Cohen*, 337 F.3d 1024, 1029 (9th Cir. 2003).

Unlike the trespass to chattels claim, the plaintiffs' conversion claim rests on the premise that their health information is property under California law. For the reasons already discussed, that is a tenuously supported legal conclusion that the Court does not need to accept as true at the pleading stage.

California Comprehensive Computer Data Access and Fraud Act. The CDAFA is California's computer crime law that prohibits the "tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a). To have standing to bring a civil claim under CDAFA, an individual must have suffered "damage or loss by reason of a violation" of the statute. *Id.* at § 502(e)(1).

The plaintiffs allege that Google source code and cookies is a "contaminant" under CDAFA and that the placement of the source code on plaintiffs' computers allowed for the taking and use of plaintiffs' data in violation of the law. *See* Dkt. No. 86 at ¶¶ 509-14. Similar to

the trespass to chattels claim, the plaintiffs' alleged damage is reduced storage, disk space, and performance of their computers and interference with their ability to communicate with their health care providers through their websites. The plaintiffs also allege loss by way of their expenditure of time and resources to investigate Google's conduct.

For the reasons already stated, the plaintiffs' allegations of lost storage, disk space, and performance, and their alleged inability to communicate with their providers, are inadequately pled. CDAFA allows compensatory damages for "any expenditure reasonably and necessarily incurred" by the computer owner "to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted" by unlawful access. Cal. Penal Code § 502(e)(1). But the plaintiffs make only a conclusory allegation that they expended time and resources to investigate Google's conduct. And, as Google rightly points out, there is no allegation that the investigation was undertaken to verify that their "data was or was not altered, damaged, or deleted."

Breach of Express Contract. A breach of contract claim under California law requires (1) the existence of a contract, (2) the plaintiff's performance or excuse for nonperformance of its side of the agreement, (3) the defendant's breach, and (4) damage to the plaintiff as a result. *See In re Facebook, Inc., Consumer Privacy User Profile Litigation*, 402 F. Supp. 3d 767, 801 (N.D. Cal. 2019).

The plaintiffs bring this claim only on behalf of plaintiffs who are Google account holders. They allege that the contracts at issue are Google's Terms of Service and Privacy Policy, which every Google account holder must agree to as a condition of opening a Google account. Although the alleged wrongdoing occurred on third-party websites, the plaintiffs note that both the Terms of Service and Privacy Policy apply because the two contracts, when read together, define Google's relationship with Google account holders when they interact with Google services, inclusive of "products that are integrated into third-party apps and sites, like ads

[and] analytics."[5]

There are four specific promises that the plaintiffs allege Google broke. First, they allege Google did not follow through on its promise to enforce rules of conduct that prohibit violating laws and privacy rights. *See* Dkt. No. 86 at ¶¶ 289, 535, 540. The plaintiffs seize on language in the Terms of Service mandating that everyone using Google's services "respect the rights of others, including privacy and intellectual property rights." Dkt. No. 86-41 at 5. The breach, according to the plaintiffs, is that Google permitted its services to be used by health care providers in ways that violate applicable laws and privacy rights. But the promise at issue is a promise that the users of Google's services make, not one that binds Google.

The second alleged breach involves Google's promise to collect only health information that users choose to provide. *See id.* at ¶¶ 536, 541. The Privacy Policy contains a section titled "Categories of information we collect" and one of the categories is "Health information." Dkt. No. 86-42 at 18-19. Within this category, Google states that information "such as your medical history, vital signs and health metrics (like blood glucose levels), and other similar information related to your physical or mental health" is collected "if you choose to provide it." The problem for the plaintiffs is that, as already outlined, they have not adequately alleged that the data transmitted to Google contains their private health information like treatments and doctors.

Third, the plaintiffs allege Google broke its promise to not use health information for personalized advertising. *See* Dkt. No. 86 at ¶¶ 537, 542. In the Privacy Policy, Google says that it does not "show personalized ads based on sensitive categories like race, religion, sexual orientation, or health." Dkt. No. 86-42 at 31. None of the plaintiffs allege they received any personalized advertisement based on their health information. Instead, the plaintiffs try to argue that Google breached this promise by building and refining its advertising systems with the plaintiffs' health information. And then they completely jump the shark by arguing that "a

[5] At the hearing, Google's counsel more or less conceded that the Terms of Service and Privacy Policy "applies to data in Google's possession if it's been shared with Google by a third party . . . ."

decision *not* to show Plaintiffs particular ads based on their health status is just as 'personalized' a misuse of their data." Dkt. No. 97 at 33. Google promised not to show personalized ads based on health, and the plaintiffs fail to allege they received any personalized ads based on their health.

Fourth, the plaintiffs allege that Google promises to use the information it receives from third parties to protect Google users from fraud and abuse. *See* Dkt. No. 86 at ¶ 289, 538; But the language the plaintiffs rely on does not say that. Google states that it uses information shared with it to maintain and improve its services, develop new services, and "protect against fraud and abuse." *See* Dkt. No. 86-51 at 2. Read in context, Google's statement to use information shared with it to "protect against fraud and abuse" implies that it is protecting its own services. There is nothing suggesting that Google is promising to prevent or protect Google users from third-party fraud or abuse.

Because the plaintiffs have failed to adequately allege Google broke any of its alleged promises in its Terms of Service or Privacy Policy, they have failed to state a claim for breach of express contract.

Breach of Implied Contract. An implied breach of contract claim has the same elements as an express breach of contract claim except its existence and terms are manifested by conduct, not words. *See California Spine & Neurosurgery Institute v. United Healthcare Insurance Co.*, No. 19-CV-02417-LHK, 2019 WL 4450842, at *3 (N.D. Cal. Sept. 17, 2019); *see also* Cal. Civ. Code § 1621. The plaintiffs allege an implied contract claim "to the extent that Google's Terms of Service and policy documents are not express contracts." But an implied contract cannot exist when there is an express contract between parties covering the same subject. *See Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1095 (N.D. Cal. 2022). Even the plaintiffs' counsel at the hearing acknowledged "we have some issues on the implied contract claim" and "maybe it's not a breach of implied contract. Maybe it's the unjust enrichment claim." The plaintiffs breach of implied contract claim is dismissed.

Breach of Implied Covenant for Good Faith/Fair Dealing. There is an implied duty in

every contract that each party must engage in good faith and fair dealing in the performance and enforcement of the contract. *See Careau & Co. v. Security Pacific Business Credit, Inc.*, 222 Cal. App. 3d 1371, 1393 (1990). The duty mandates "that neither party will do anything which will injure the right of the other to receive the benefits of the agreement." *Id.*

The plaintiffs allege Google violated this implied covenant by abusing "its power to define terms of the contract" such as limiting the meaning of "health information" or changing the meaning of personally identifiable information. Perhaps an objectively unreasonable interpretation of a contract term to deny one party the benefit of the bargain could form the basis for a breach of implied covenant claim. Here, however, the plaintiffs have not adequately alleged that Google's interpretation of "health information" or "personally identifiable information" is objectively unreasonable. Thus, they have failed to state a claim for breach of the implied covenant of good faith and fair dealing.

Unjust Enrichment. Under California law, unjust enrichment is "synonymous with restitution" and describes "the theory underlying a claim that a defendant has been unjustly conferred a benefit through mistake, fraud, coercion, or request." *Astiana v. Hain Celestial Group, Inc.*, 783 F.3d 753, 762 (9th Cir. 2015). The plaintiffs allege that Google has unjustly received economic benefit from its use of the plaintiffs' personal data without their consent. But because the plaintiffs have not stated a claim against Google for any unlawful conduct, they have also failed to state an unjust enrichment claim.

IV.

In this case, the plaintiffs appear to have chosen a strategy often used in securities fraud cases: If you make the complaint incredibly long and attach tons of exhibits, maybe a court will be more inclined to think the claims are pled with sufficient plausibility and specificity. That's usually a bad strategy, and it was a bad strategy here. The length of the complaint, and the number of exhibits attached, made the plaintiffs' presentation difficult to follow, not to mention self-contradictory. And despite the complaint's length, the most important allegations were conclusory. It would be reasonable, considering the number of chances the plaintiffs have

already been given, to dismiss the complaint with prejudice. But the plaintiffs will get one last chance, and dismissal is with leave to amend. One thing is for sure: if the next iteration of the complaint is remotely close to 188 pages, the plaintiffs will only be hurting their chances.

Any amended complaint is due within 21 days. If no amended complaint is filed by that deadline, dismissal is with prejudice. If an amended complaint is filed, Google's response is due 21 days later.

IT IS SO ORDERED.

Dated: July 22, 2024

VINCE CHHABRIA
United States District Judge