

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 IN PART,
DENYING IN PART, MOTION TO
DISMISS SECOND AMENDED
COMPLAINT**

Re: Dkt. No. 164

The first amended complaint was dismissed for a number of related reasons, but mostly because it failed to adequately allege that Google was intentionally receiving communications between health providers and patients that contained private health information that could be connected to an identifiable person. *See Doe I v. Google LLC*, 741 F. Supp. 3d 828 (N.D. Cal. 2024). In the second amended complaint, the plaintiffs have improved their allegations (as well as their explanation of those allegations). These improvements get them barely over the line in alleging that Google, until some point in 2023, intentionally obtained this type of communication. But in 2023, Google started giving clear instructions to its health-provider clients, explaining how to avoid sending private health care information to Google, and emphasizing that Google didn't want that information. The allegations in the complaint do not support an inference that Google, after this point, intentionally obtained communications containing private health information about identifiable patients. Section I discusses the issue of intent, and Section II goes through the various claims contained in the second amended complaint. This ruling assumes the reader is familiar with the complaint, the briefs, the transcript

of the hearing, and the Court’s ruling on the previous iteration of the complaint.¹

I

As a preliminary matter, there is no dispute that Google received *some* communications between health providers and users of the providers’ websites. That’s the point of Google’s products—the source code is designed to collect and analyze communications on the webpages on which it is enabled.

Moreover, the complaint has adequately alleged that some of the provider-patient communications Google received contained the kind of private health information that is protected under federal law. Under HIPAA, private health information “relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.” 42 C.F.R. § 160.103; 42 U.S.C. § 1320d(4).² The plaintiffs adequately allege that health information is collected by Google when a patient does a variety of things on a provider website—looks up information about their diagnosis, searches for practitioners who treat the patient’s medical condition, attempts to make an appointment online with those practitioners, or tries to pay bills to the provider online—and Google Source Code is enabled on the webpages where those activities occurred. For example, one screenshot provided from the plaintiffs’ investigation identifies an “event” collected by Google showing that the user clicked on the “make appointment” button for a urologist. Ex. 1 to SAC at 5, Dkt. No. 159-4. If a user has a urinary tract infection and Google collects information that the user is looking up urologists, booking appointments, searching for information about urinary tract infections and how to treat them, and navigating to the “bill pay” screen, that would be plenty to draw the communications under the umbrella of “health information,” i.e., information that “relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an

¹ Google’s request for judicial notice is granted, except as to disputed exhibits 6, 7, 8, and 9, because those documents are not necessary for the resolution of this motion.

² The FTC uses the same definition. 16 C.F.R. § 318.2.

individual, or the past, present, or future payment for the provision of health care to an individual.” 42 C.F.R. § 160.103; 42 U.S.C. § 1320d(4). And the plaintiffs allege specifically that they had certain conditions and saw certain practitioners. SAC at ¶¶ 38, 45–46, 54, 60, 67, 74. They then allege they conducted searches on the providers’ websites for how to treat those conditions, looked for practitioners, and navigated to the bill pay webpage. *Id.*

The plaintiffs have also adequately alleged that the information collected by Google can be tied to a particular person—to use common parlance, the information is “individually identifiable.” Again, they tie their allegations to HIPAA, which says that information is individually identifiable if “there is a reasonable basis to believe the information can be used to identify the individual.” 45 C.F.R. § 160.103. The plaintiffs allege that Google obtains communications between provider and patient by collecting URLs, cookies, and substantive events that occur on the providers’ webpages and sending them to Google-owned endpoints. SAC at ¶¶ 24–29. In addition, according to the complaint’s allegations, Google always collects the Internet Protocol (IP) address of the user when it captures a communication on a webpage. *Id.* at ¶¶ 91–102. Thus, under the plain language of the relevant HIPAA regulations, all of the information at issue here was identifiable.³ See 45 C.F.R. § 165.514(b)(2)(i)(O) (noting that, for health information to be considered de-identified, IP addresses must be removed). And certainly it would be reasonable to infer that Google, out of anyone, would be able to use an IP address to connect information to an identifiable person. As the plaintiffs point out, Google has access to vast amounts of information through its various products, and because the range of information collected by those products is so broad, it’s plausible that Google would know enough about the

³ Google cites *American Hospital Association v. Becerra* for the proposition that website tracking of searches for medical issues on unauthenticated pages does not automatically result in tracking of individually identifiable health information because a user might have visited a webpage for research or for a hypothetical purpose. 738 F. Supp. 3d 780, 788–91 (N.D. Tex. 2024). But the posture of that case was much different than this one. That case was an APA challenge to HHS guidance based on the scope of HIPAA, regarding HHS’s authority to promulgate that guidance. This case is brought by patients who allege that they have *current* conditions and that their activity on the providers’ websites were “related to” those diagnoses. See, e.g., SAC at ¶ 67 (plaintiff with kidney issues searched for nephrologist).

activity of an IP address to be able to tie it to an identifiable person, say, through the information that person provides while setting up a Google account or shopping on another website. SAC at ¶¶ 104–108.

Google contends that the plaintiffs should be required to allege that Google actually identified the user attached to the communication. But HIPAA does not require that the person actually be identified for their personal health information to be considered individually identifiable. Instead, HIPAA only requires “a reasonable basis to believe the information can be used to identify the individual.” 45 C.F.R. § 160.103. This is consistent with common sense—if you obtain someone’s communication, and that communication contains private health information about them, and you have the ability to figure out who the person is, then you’ve obtained private information about them in a way that infringes on their privacy interests. At least if you obtained the communication intentionally.

And that’s the next question—whether the plaintiffs have adequately alleged that Google intended to collect these communications. As mentioned, Google obviously intended to collect *some* communications between patient and provider: the whole point of the products at issue is for Google to help the providers curate and utilize information about these communications. But this lawsuit seeks to impose liability on Google only for the collection of communications that contain individually identifiable health information as defined by HIPAA (and as similarly defined by the FTC). So the question is not whether Google intended to collect any old communication. The question is whether Google intended to collect the kinds of communications at issue in this lawsuit.

Based on the allegations in the complaint and the materials that can be considered at the pleading stage, the answer to this question depends on the time period. At some point in 2023, apparently in response to growing concerns about Google and other pixel firms obtaining people’s private health information, Google updated its help pages to explain to providers (and other customers) how they can and must avoid sending health information to Google. For starters, Google explained that protected health information under HIPAA might be different

than personally identifiable information as defined by Google’s policies. It went on to explain that customers “may only use Google Analytics on pages that are not HIPAA-covered,” and urged customers to avoid putting Google Analytics tags on both authenticated websites and certain unauthenticated websites related to the provision of health information. Dkt. No. 165-3. That language creates only one plausible inference: Google, aware of how its products operate and the information that it is constantly collecting regardless of selection by its customers, took measures to prevent itself from receiving communications containing private health information by clearly instructing health providers not to put Google Analytics on the wrong webpages. And as discussed in the prior ruling, to the extent the plaintiffs argue that this was all just a ruse, their allegations don’t support that inference, regardless of which pleading standard applies to this allegation. *Doe I*, 741 F. Supp. 3d at 841–42.

But with respect to information collected prior to the 2023 warning, it’s reasonable to infer from the allegations in the complaint and the materials that can be considered at this stage that Google intended to receive communications containing individually identifiable health information. Google’s prior language vaguely stated that providers “may not use Google Analytics for any purpose or in any manner involving Protected Health Information unless you have received prior written consent to such use from Google.” Ex. 4 to Request for Judicial Notice at 3, Dkt. No. 165-5. At least based on the allegations in the complaint, anyone familiar with how the products operate would likely know that this warning is so inadequate that at least some clients would inevitably use the products in a way that would cause the unwitting transmission of communications containing individually identifiable health information. Against this factual backdrop, it would be reasonable to infer that Google was engaged in an affirmative effort to obtain these communications. The Court is skeptical of this theory—it seems much more likely that the evidence will ultimately reflect negligence or recklessness on Google’s part, not an intent to have clients using the products in a way that would cause the transmission of communications containing private health information. But judicial skepticism is not a reason to throw out the claims. *See Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 556 (2007). And it’s

plausible to infer, given how obvious this problem was before 2023, that Google actually intended to capitalize on the problem.

Accordingly, to the extent that the plaintiffs' claims under the Wiretap Act, CIPA, intrusion upon seclusion, and common law privacy can survive this motion to dismiss, it would only be for communications obtained before the publication of the updated language in 2023. Each claim for that period is discussed in the next section.

II

1. *Wiretap Act*: Google argues that, because the providers installed Google's products on their websites, they consented to the interception of the plaintiffs' communications. But based on the discussion above, a plausible inference is that while the providers consented to the installation of Google's Source Code, they did not consent to the collection of individually identifiable health information because they did not understand (at a minimum) that automatic collection of certain information, such as IP address, was rendering the communications "individually identifiable" under HIPAA.⁴ So consent is a factual issue that cannot be resolved on the pleadings.

2. *Section 631 of CIPA*: Google asserts that it merely functioned as an extension of the providers' websites and thus should not be considered liable as a third-party vendor. *See Williams v. What If Holdings, LLC*, 2022 WL 17869275, at *3 (N.D. Cal. Dec. 22, 2022); *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 833 (N.D. Cal. 2021); *Rodriguez v. Ford Motor Co.*, 722 F. Supp. 3d 1104, 1117–22 (S.D. Cal. 2024) (collecting cases). But the plaintiffs now plausibly allege that Google uses the data collected from health providers for its own purposes, including by using the information to improve its products. SAC at ¶¶134–44.

In addition, Google argues that the data sent to Google were not the "contents" of a communication. But the URLs collected contained "both the path and the query string," which

⁴ While the plaintiffs argue that the crime-tort exception should apply, they have not alleged facts (under any pleading standard) sufficient to create an inference that the providers were in cahoots with Google for Google to intercept health information in violation of HIPAA.

were the “contents” of a communication “because they concern the substance of a communication.” *Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1077 (N.D. Cal. 2023), motion to certify appeal denied, No. 22-CV-03580-WHO, 2024 WL 4375776 (N.D. Cal. Oct. 2, 2024) (citing *In re Zynga Privacy Litigation*, 750 F.3d 1098, 1106 (9th Cir. 2014)); *see* SAC at ¶ 76 (alleging that <https://www.eehealth.org/services/behavioral-health/programs/eating-disorders/> was collected by Google). In addition, a button-click for “bill pay” would seem to be the content of a communication because the user was trying to substantively communicate with the provider.

3. *Section 632 of CIPA*: Google argues that the plaintiffs have failed to establish that Google, as opposed to the providers, “recorded” the data. But while the providers in some circumstances chose which events to capture, Google did the actual recording, and the plaintiffs allege that Google sent all interceptions to Google endpoints and then used the information for its own purposes.

Google also asserts that no reasonable person would believe that the communications captured were confidential because the providers were required to disclose their use of Google Analytics. But at this stage the Court is unable to determine whether the disclosures were sufficiently clear, such that it is implausible that a reasonable person would have an expectation of privacy in their interactions on the providers’ websites.

4. *Intrusion Upon Seclusion / Common Law Privacy*: First, Google contends that the Terms of Service, which required that providers disclose the use of Google Analytics, shows that there was no intent to intrude on a communication in which the plaintiffs had a reasonable expectation of privacy. But as noted above, the intent question goes to the plaintiffs, at least at the pleading stage, before Google began properly instructing clients on how to avoid HIPAA violations.

Second, Google argues that there is no reasonable expectation of privacy in the data it collected because the visitor’s intent, i.e., why they were accessing the specific webpages at issue, was not discernable by Google. But a reasonable person, knowing their own medical

diagnoses, would have a reasonable expectation of privacy as to their website searches relating to those diagnoses on their healthcare providers' websites.⁵

Finally, Google argues that the plaintiffs cannot establish that the intrusion was highly offensive. But the plaintiffs have plausibly alleged that Google collected their private health information, which is enough at this stage.

5. Breach of Contract: As to the first promise, the plaintiffs have stated a claim for breach of contract with Google accountholders. A reasonable person could conclude that Google promised not to collect Google users' health information outside of the specific instances identified in Google's Terms of Service and Privacy Policy. In its Privacy Policy, Google announces that it will collect information about users' activities in its services, including “[a]ctivity on third-party sites and apps that use our services.” Dkt. No. 158-14 at 3. This is not in reference to health information, but to information generally. Later, the policy discusses different categories of information that will be collected. This includes health information “if you choose to provide it . . . in the course of using Google services that offer health-related features, such as the Google Health Studies app.” *Id.* at 18. These two provisions, read together, are best understood (at least at the pleading stage) as promising not to collect private health information except in those limited circumstances.

As to the second promise, however, the plaintiffs have failed to state a claim. They allege that Google breached its promise not to use health information in personalized advertising. *Id.* at 30 (“We don’t use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we require the same from advertisers that use our services.”). But the help pages cited by the plaintiffs tend to support Google’s assertion that it does not use health information in its personalized advertising business. *See* Ex. 5 to Google’s

⁵ Google cites *Smith v. Facebook, Inc.*, for the proposition that viewing publicly available health information is not the type of sensitive communication in which one would have a reasonable expectation of privacy. 745 F. App’x 8, 9 (9th Cir. 2018). But in *Smith*, the Ninth Circuit was considering whether the data collected was so sensitive that it should be considered outside of the plaintiffs’ consent to tracking. *Id.*

Request for Judicial Notice at 3–4, Dkt. No. 165-6. And none of the plaintiffs allege that they received any ads related to their browsing activity. This claim is dismissed with prejudice.

6. *Breach of Implied Covenant for Good Faith/Fair Dealing*: The plaintiffs continue to fail to state a claim for breach of the implied covenant, as discussed in the previous order. *Doe I*, 741 F. Supp. 3d at 848. This claim is dismissed with prejudice.

7. *Unjust Enrichment*: This claim can move forward because the plaintiffs have now plausibly alleged that Google acted unlawfully in collecting their health information, and that Google derived value from the use of the plaintiffs' health information. While Google argues that the plaintiffs' unjust enrichment claim cannot be sustained because the plaintiffs also allege the existence of a valid express contract covering the same subject matter, the plaintiffs are permitted to plead their unjust enrichment claim in the alternative to the breach of contract claim. *See In re Facebook, Inc., Consumer Privacy User Profile Litigation*, 402 F. Supp. 3d 767, 803 (N.D. Cal. 2019).

* * *

To summarize: The plaintiffs' claims under the Wiretap Act, CIPA, intrusion upon seclusion, and common law privacy are dismissed for communications occurring after Google updated its help pages in 2023, but can go forward for claims based on communications before that point. The plaintiffs' breach of contract claim is dismissed in part, and the claim for breach of implied covenant is dismissed in full. All dismissals are with prejudice. A case management conference is set for July 11 at 10:00 am on Zoom for this case and the related case, *Newton v. Google*, Case No. 25-cv-570.

IT IS SO ORDERED.

Dated: June 6, 2025



VINCE CHHABRIA
United States District Judge