UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

Daniel Cancelmo, on behalf of himself
and all others similarly situated

v.

Case No. 24-cv-245-SE
Opinion No. 2025 DNH 122

Southern New Hampshire Medical Center,
et al.

O R D E R

Daniel Cancelmo, on behalf of himself and a putative class, brings suit against Southern New Hampshire Medical Center, Southern New Hampshire Health System, Incorporated, and SolutionHealth, alleging that the defendants unlawfully shared Cancelmo's and class members' health information with Google and used Google software to record that information. He brings one claim under Revised Statutes Annotated (RSA) 332-I:4, I, which regulates the use and disclosure of protected health information for marketing purposes, and the other under the New Hampshire Wiretap Act, RSA 570-A. The defendants move to dismiss both claims.

Standard of Review

To survive a Rule 12(b)(6) motion to dismiss for failure to state a claim, a plaintiff must make factual allegations sufficient to "state a claim to relief that is plausible on its face." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)). A claim is facially plausible if it pleads "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. This standard "demands that a party do more than suggest in conclusory terms the existence of questions of fact about the elements of a claim." A.G. ex rel. Maddox v. Elsevier, Inc., 732 F.3d

77, 81 (1st Cir. 2013). To test a complaint's sufficiency, the court must employ a two-step approach. First, it must identify and disregard statements that "merely offer 'legal conclusions couched as fact' or 'threadbare recitals of the elements of a cause of action.'" Ocasio-Hernández v. Fortuño-Burset, 640 F.3d 1, 12 (1st Cir. 2011) (quoting Iqbal, 556 U.S. at 678 (alterations omitted)). Second, the court must credit as true all nonconclusory factual allegations and the reasonable inferences drawn from those allegations. See id. Only then can the court determine whether the "combined allegations, taken as true, . . . state a plausible, not a merely conceivable, case for relief." Id. (quotation omitted).

Background

The defendants own, operate, or manage hospitals in southern New Hampshire. As part of their services, the defendants provide a website that is accessible to those who "are or were patients or prospective patients." Doc. no. 1-1, ¶ 19. Website visitors can use the website in a variety of ways. For example, they can "log in to the Patient Portal," pay bills, make appointments, and perform search queries, sometimes through the homepage, for doctors by specialty, gender, location, and availability. Id., ¶¶ 20, 35, 37, 40-41. The allegations specific to Cancelmo, as opposed to those concerning the putative class, involve only the unauthenticated public webpages, or pages that do not require a user to log in.

The defendants shared information about visitors' interactions on their website with Google Analytics, a program designed by Google. Cancelmo alleges that the defendants shared different types of information with Google without users' consent, including: searches for medical treatment; the name, gender, and specialty of physicians with whom patients are seeking treatment; portal log-in times and locations; searches on the site's search bar; and Internet

Protocol (IP) Addresses. "An IP address is a number that identifies an individual's device connected to the internet and can be used to gather insights about their online activity and geographic location." Id., ¶ 22.

In their Terms of Use (Terms), the defendants acknowledge that they use "Google AdWords remarketing service" with the "intent to retarget website visitors." Id., ¶ 30. However, users "are not required to consent to the site's Terms, nor are they presented with the Terms at any stage as they browse the website." Id. In fact, to view the Terms, a user would need to "scroll to the bottom of the page and voluntarily find and select the Terms hyperlink, which is displayed in smaller font than almost all other text on the page." Id.

Cancelmo sued the defendants in New Hampshire state court on behalf of himself and a putative class of "approximately tens of thousands" of other users for violating state laws related to protecting privacy. Id., ¶ 4. Shortly thereafter, the defendants removed the case to federal court under the Class Action Fairness Act, 28 USC §§ 1332(d), 1453. Doc. no. 1. They then filed a motion to dismiss (doc. no. 7) to which Cancelmo objected (doc. no. 14).

Discussion

Cancelmo brings two claims under New Hampshire state law. He alleges that the defendants violated RSA 332-I:4, I (Count I), which prohibits the unauthorized disclosure of medical information for marketing purposes (with some exceptions that are not relevant here); and that the defendants violated the Wiretap Act (Count II). As a federal court applying New Hampshire law, this court endeavors to interpret New Hampshire statutes as the New Hampshire Supreme Court would interpret them. See Bourgeois v. TJX Comps., Inc., 129 F.4th 28, 33 (1st Cir. 2025).

I. RSA 332-I (Count I)

Cancelmo alleges that the defendants violated RSA 332-I:4, I, by sharing users' website interactions with Google Analytics, which in turn uses those interactions to market the defendants' services back to those same users. In relevant part, RSA 332-I:4, I, states: "A health care provider, or a business associate of the health care provider, shall obtain an authorization for any use or disclosure of protected health information for marketing." Though no court—New Hampshire, federal, or otherwise—appears to have addressed RSA 332-I:4, I, the parties agree that this provision requires Cancelmo to allege, at the very least, that the defendants (1) used or disclosed (2) protected health information (3) for marketing. The defendants dispute that Cancelmo has alleged any of these elements as to either himself, as he must, or as to putative class members.

A. Allegations Related to Cancelmo

"Class actions are useful to remedy widespread wrongs, but such lawsuits still require at the outset a viable named plaintiff with a plausible claim." Pruell v. Caritas Christi, 678 F.3d 10, 14 (1st Cir. 2012). When, as here, no class has been certified, the court considers only Cancelmo's claims on his own behalf, rather than on behalf of the putative class. See Moore v. Metro. Grp. Prop. & Cas. Ins. Co., No. CA 10-212ML, 2010 WL 5069856, at *2 (D.R.I. Dec. 6, 2010) (considering only the named plaintiff's claims because "no class has been certified by this Court pursuant to Rule 23 of the Federal Rules of Civil Procedure"); Simonet v. SmithKline Beecham Corp., 506 F. Supp. 2d 77, 81 (D.P.R. 2007) ("At [the precertification] stage of the litigation, the court must dismiss

the complaint in its entirety if the named plaintiff has no cause of action in her own right."); Evans v. Taco Bell Corp., No. CIV. 04CV103JD, 2005 WL 2333841, at *4 (D.N.H. Sept. 23, 2005) ("But unless and until the court certifies such a class, the potential claims of putative class members other than the named plaintiff are simply not before the court."); see also Police & Fire Ret. Sys. of Detroit v. IndyMac MBS, Inc., 721 F.3d 95, 112 n.22 (2d Cir. 2013) (noting "until certification there is no class action but merely the prospect of one; the only action is the suit by the named plaintiffs" (quoting Morlan v. Universal Guar. Life Ins. Co., 298 F.3d 609, 616 (7th Cir. 2002))).

Although the complaint contains several instances of exemplar searches by fictitious patients, the allegations regarding Cancelmo himself are sparse. The complaint alleges that Cancelmo used the defendants' "website on multiple occasions to search for medical providers and their contact information, including but not limited to the [defendants'] allergy clinic and dermatology services." Doc. no. 1-1, ¶ 20. The complaint also alleges that Cancelmo used the "Find a Doctor" feature to search for a male doctor who is accepting new patients and who specializes in dermatology, and that the defendants transmitted to Google that Cancelmo used that feature and the "Make an Appointment" feature on its website.[1] Id., ¶¶ 40-41.

These allegations are not sufficient to allege plausibly the elements of a claim under RSA 332-I(4), I. Again, as the parties agree, a claim under that statute requires allegations that the defendants (1) used or disclosed (2) protected health information (3) for marketing.

[1] Cancelmo did not point to these allegations as specific to his own activity when he addressed the defendants' arguments in his objection. Nevertheless, these allegations appear to be attributed to Cancelmo, rather than exemplar searches discussed elsewhere in the complaint.

With regard to Cancelmo, it is questionable whether he has alleged that the defendants disclosed his protected health information. RSA 332-I ties the definition of "protected health information" to federal regulations under HIPAA. RSA 332-I:1, II(a)(4). Under HIPAA, "protected health information" is "individually identifiable health information" that is "transmitted or maintained" in any form. 45 CFR 160.103. In turn, individually identifiable health information is, in relevant part, information that (1) "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," and (2) "identifies the individual or . . . with respect to which there is a reasonable basis to believe the information can be used to identify the individual." Id. First, Cancelmo does not allege that he had a medical need for a dermatologist, made an appointment with one, or intended to make an appointment. Thus, it is not clear that Cancelmo's use of the unauthenticated public webpages satisfies the first part of the definition.

As to the second part of the definition, HIPAA regulations suggest that IP addresses are considered individually identifying markers, 45 C.F.R. § 165.514(b)(2)(i)(O), though that point is somewhat in dispute, see Am. Hosp. Ass'n v. Becerra, 738 F. Supp. 3d 780, 789 (N.D. Tex. 2024) (vacating a Department of Health and Human Services guidance that stated that HIPAA obligations can attach to "online technology" that connects an individual's IP Address to their visits to certain public webpages). Here, assuming without deciding that IP addresses are considered individually identifying information, the complaint does not allege that the defendants used or disclosed that information with regard to Cancelmo. The complaint offers several examples of other exemplar patients' searches on the defendants' website, and states that the "information, combined with the patient's IP address which is also shared in all these

example cases, enable Google to identify the individual who has submitted this information through the [defendants'] website." Doc. no. 1-1, ¶ 39. But such allegations are absent with regard to Cancelmo's own search.

More importantly, however, missing from the complaint is any allegation that the defendants used or disclosed Cancelmo's private health information for marketing. Cancelmo alleges generally that the "presence of active campaigns on Google Ads establishes a direct connection between [the defendants'] data-sharing practices and its ongoing marketing efforts." Id., ¶ 66. The complaint includes undated screenshots of advertisements for the defendants' services. Id. But even if the court credited the allegation that the presence of such ads showed that the defendants shared information with Google for marketing purposes, none of those allegations is related to Cancelmo's search. Although many of the advertisements are directed toward specialty care, including weight loss and surgery, pediatric, and urgent care, none pertains to dermatology or allergies. Id. Therefore, Cancelmo has not sufficiently alleged that the defendants disclosed his information, private or otherwise, for marketing.

For these reasons, the complaint does not allege a plausible claim for relief in Count I with regard to Cancelmo. Therefore, the court dismisses Count I, though it does so without prejudice to Cancelmo's right to amend his complaint.

B. Remaining Arguments as to Count I

Because the court grants the defendants' motion to dismiss as to Count I for the reasons stated, it does not address their remaining arguments as to that count. The court now turns to Count II.

II. New Hampshire Wiretap Act (Count II)

Cancelmo also alleges that the defendants violated the Wiretap Act. The complaint does not specify under which provision Cancelmo brings his claim. In their motion to dismiss, the defendants construe Cancelmo's claim under either RSA 570-A:2, I(a) (the Interception Provision), or RSA 570-A:2, I(c) (the Disclosure Provision).[2] In his objection to the motion to dismiss, Cancelmo focuses primarily on the Interception Provision, see doc. no. 14 at 20-21 (quoting RSA 570-A:2, I(a)); however, he also objects to the defendants' arguments with respect to the Disclosure Provision, id. at 23-25 (citing RSA 570-A:2, I(c)). The court addresses the arguments relating to both provisions, concluding that Cancelmo has adequately alleged claims under each.

A. The Interception Provision

The Interception Provision makes it illegal to (1) "wilfully intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept," (2) "any telecommunication or oral communication" (3) "without the consent of all parties to the communication." RSA 570-A:2, I(a). Cancelmo asserts that the defendants violated this provision by using Google Analytics to record his interactions with their website.

The defendants argue that Cancelmo's complaint alleges none of the requisite elements of the Interception Provision. First, they argue that the information communicated through their website is not a telecommunication under the statute. Second, they argue that Cancelmo has not alleged that they "intercepted" information. And third, they argue that Cancelmo and other

[2] Though RSA 570-A is a criminal statute, it provides for both criminal penalties and a civil remedy for Wiretap Act violations. RSA 570:11.

website visitors "inherently consent" to the defendants' use of Google Analytics to memorialize user interactions with their website. Doc. no. 7-1 at 22. The court takes each argument in turn.

1. Telecommunication

To bring his claim under the Wiretap Act, Cancelmo must adequately allege that his interactions with the defendants' unauthenticated public webpages are telecommunications. The Wiretap Act defines a "telecommunication" as "the transfer of any form of information in whole or in part through the facilities of a communications common carrier." RSA 570-A:1, I. Cancelmo's allegations satisfy this definition. Cancelmo "transfer[red] . . . information" to the defendants when he searched for medical providers and accessed the "make an appointment" feature on the website. See, e.g., doc. no. 1-1, ¶¶ 20, 40-41.

Nevertheless, the defendants argue that the complaint does not allege a telecommunication for two separate reasons. First, the defendants seize on the fact that Cancelmo's complaint repeatedly describes Google Analytics as a "tracking technology" or a "tracking tool." Thus, they argue, Google Analytics falls outside the definition of a "telecommunication," which excludes "any communication made . . . from a tracking device." RSA 570-A:1, I. Even assuming that Google Analytics is a tracking device, this argument fails because it misunderstands Cancelmo's theory under the Interception Provision. For Cancelmo, the alleged telecommunications that the defendants intercepted are his website interactions—i.e., his searches. These interactions originate from Cancelmo, not from Google.

Regardless, the court finds unpersuasive the defendants' argument that Google Analytics is a "tracking device" excluding it from the definition of "telecommunication" under the statute. Cancelmo's use of the terms "tracking technology" and "tracking tool" in the complaint is

irrelevant. As a matter of statutory interpretation, the court finds it far more plausible that "tracking device" refers to the type of device that can follow a person's location, and not a type of software that can track a user's internet activity. This is especially true given the fact that the statute was last amended in 1995, well before such software or activity became generally available. Thus, Cancelmo's allegations do not fall into the statutory exclusion for tracking devices.

Second, in their reply brief, the defendants argue that a "telecommunication" must be "person-to-person." To support this argument, they point to a recent decision of the Massachusetts Supreme Judicial Court (SJC), Vita v. New England Baptist Hospital, 494 Mass. 824 (2024). In Vita, the SJC addressed a claim similar to Cancelmo's. Id. at 825. At issue in Vita was whether "wire communications" under the Massachusetts Wiretap Act encompassed user interactions with two hospitals' websites. Id. at 825-26. The Massachusetts Wiretap Act protects oral and wire communications. G. L. c. 272, § 99 C 1. It defines "wire communication" as "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception." G. L. c. 272, § 99 B 1. Analyzing the text of the statute, the court decided that the undefined term "communication" was ambiguous with respect to web browsing, noting in the process that it had never been applied to activities that did not include "person-to-person" communications. Id. at 834-47. In light of this ambiguity and the fact that violations of the Massachusetts Wiretap Act can carry criminal penalties, the SJC applied the rule of lenity, which counsels courts to interpret ambiguous criminal statutes in favor of defendants, and declined to extend the law to website interactions. Id. at 847-48.

This court respectfully declines to apply Vita because the New Hampshire Wiretap Act is distinguishable. Unlike the Massachusetts Wiretap Act, which is ambiguous because it does not define "communication[s]," the New Hampshire Wiretap Act is not ambiguous because it protects "telecommunication[s]," which it defines as "the transfer of any form of information in whole or in part through the facilities of a communications common carrier."[3] There is no dispute that the activity alleged in the complaint satisfies this definition. Nevertheless, the defendants ask the court to limit the application of the statute to person-to-person communications notwithstanding the statute's plain language.

In State v. Lott, the New Hampshire Supreme Court held that an interception under the Wiretap Act occurred when an instant messaging program recorded messages sent between two users of that program and displayed those messages in the respective users' chat windows. 152 N.H. 436, 438-39 (2005). In reaching this conclusion, the court elucidated its approach to interpreting the Wiretap Act:

> We recognize that the statutory definitions of "intercept" and "electronic, mechanical, or other device" have not changed in any meaningful way since 1988, when internet communications technology was in a nascent stage of development. Although the prevalence of internet communications technology has expanded rapidly since that time, and although the statute might appear outdated, when, as here, the language of the statute is plain and unambiguous, we are bound by that language, and do not add words that the lawmakers have not seen fit to add, nor consider what the legislature might have said were it presented with the facts before us in this case.

Id. at 439.

Applying these principles, the court finds it inappropriate to limit the statute as the defendants request. Focusing on the text as written, nothing in the definition of

[3] At this stage of the proceedings, the defendants evidently do not dispute that the internet service providers involved in the website activity at issue in this case are "communications common carriers" for the purpose of the statute.

"telecommunications" requires that such transfers of information be between two people. "Telecommunications" is defined to encapsulate "the transfer of *any* form of information in whole *or in part*." RSA 570-A:1, I (emphasis added). Rejecting the defendants' arguments to the contrary, the court finds that Cancelmo has alleged a telecommunication under the Wiretap Act.

2. Interception

The defendants also argue that Cancelmo does not allege an "interception." Specifically, they contend that his complaint falls short because it does not assert that Google Analytics records website interactions while they are "in transit," a requirement that has been adopted by courts interpreting the federal Wiretap Act and other states' wiretap acts. Doc. no. 7-1 at 19-20; doc. no. 18 at 9; see, e.g., Glob. Pol'y Partners, LLC v. Yessin, 686 F. Supp. 2d 631, 638 (E.D. Va. 2009) ("In other words, [the federal and Virginia Wiretap Statues] give 'intercept' its common meaning, which is perhaps best understood through a football analogy. In American football, a ball can only be intercepted when it is 'in flight.'"). The defendants point out that in his complaint, Cancelmo alleges that he communicated information to the defendants, who then "transmitted" that information to Google. Doc. no. 7-1 at 20; see, e.g., doc. no. 1-1, ¶ 34. Under this arrangement, they continue, the defendants do not use Google to "intercept" Cancelmo's website interactions because Google has not been interposed between the user (the transmitter of information) and the defendant (the recipient of the information).

The defendants' reading of Cancelmo's complaint is too restricted. The complaint asserts that the defendants "embed[]" Google Analytics on their website, "thus intercepting" Cancelmo's communications. Doc. no. 1-1, ¶ 75. The defendants may be able to provide technological information in a summary judgment record to overcome these allegations, but

drawing every reasonable inference in Cancelmo's favor, as the court must do at this stage, they are sufficient. The court can reasonably infer from these allegations, coupled with Cancelmo's allegations that his search for a doctor and his use of the Make an Appointment feature were transferred to Google, that the defendants use Google Analytics to contemporaneously record user interactions with the website. In this way, Google Analytics operates much like instant messaging software that "record[s]" incoming messages just as they are "received" by a user of the program. Lott, 152 N.H. at 438; see RSA 570-A:1, III (an "interception" includes "the recording of[] the contents of any telecommunication . . . through the use of any electronic . . . device."). At this stage of the litigation, Cancelmo has adequately alleged an interception.

3. Consent

Finally, to bring a claim under the Interception Provision, Cancelmo must allege that he did not consent to the defendants' alleged interception. Relying on Lott, the defendants argue that Cancelmo and other users "inherently consented," as a matter of law, to having their data recorded whenever they used the defendants' website. Doc. no. 7-1 at 22. In addition to holding that an instant messaging program "intercepted" messages as they were communicated between two users, the New Hampshire Supreme Court held in Lott that users of this messaging software implicitly consented to these interceptions. Lott, 152 N.H. at 439, 441-42. In reaching this second conclusion, the court reasoned that "the recording of the instant message is necessary for the intended recipient of that message to read the message." Id. at 441. Thus, the Court resolved, "there is no reason to believe that a person who receives this type of instant message . . . may not

choose to preserve that communication . . . " and therefore, those who used the instant messaging software "implicitly consented to the recording of" their communications. Id. at 441-42.[4]

Cancelmo's allegations are plainly distinguishable from the relevant facts in Lott. None of Cancelmo's allegations (which the court must take as true at this stage) suggest that recording users' website interactions is necessary for the website to process them. And more importantly, there are many reasons for users to believe that the defendants would not record private health information without seeking their approval to do so. Indeed, the fact that the defendants only disclose that they use Google to record users' website interactions in their Terms, which can only be accessed by scrolling to the bottom of their home page and clicking on hyperlink in a small font, suggests that many users are not aware and have not implicitly consented. At this stage, the court declines to hold that users of the defendants' website implicitly consent to the interception of their telecommunications. Cancelmo has therefore alleged a violation of the Interception Provision.

B. The Disclosure Provision

As mentioned, it is not clear whether Cancelmo intends to bring a claim under the Disclosure Provision. Nevertheless, the court addresses the parties' arguments regarding this provision.

The Disclosure Provision makes it illegal to "[w]ilfully disclose[], or endeavor[] to disclose, to any other person the contents of any telecommunication or oral communication,

[4] The defendants also rely on State v. Moscone, 161 N.H. 355 (2011). In a single paragraph at the end of that opinion, the New Hampshire Supreme Court reaffirmed Lott and extended it to hold that even where the user of an instant messaging program asks the recipient of their messages to delete them, the user still has implicitly consented to the interception of their communication. Id. at 363. Moscone does not affect the court's analysis here.

knowing or having reason to know that the information was obtained through the interception of a telecommunication or oral communication in violation of this paragraph" "without the consent of all parties to the communication." RSA 570-A:2, I(c). Though it is far from clear, Cancelmo's theory under the Disclosure Provision seems to be that the defendants disclosed to Google the contents of his interactions with their website.

The defendants argue that Cancelmo has not alleged facts that could establish that they disclosed the "contents" of any telecommunication. Drawing from case law involving the federal and other states' Wiretap Acts, the defendants argue that "content" is limited to the "the intended message conveyed by the communication," and excludes "'record information regarding the characteristics of the message that is generated in the course of the communication' such as 'the name, address and subscriber number or identity of a subscriber or customer.'" Doc. no. 7-1 at 20-21 (quoting In re Zynga Priv. Litig., 750 F.3d 1098, 1106 (9th Cir. 2014)).

The court does not find this argument persuasive. The Wiretap Act defines "contents" more broadly than do its sibling statutes. Under the Wiretap Act, the definition of contents "includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." RSA 570-A:1, VII. That definition plainly covers the website interactions that Cancelmo alleges—the identification of a specific specialty helps describe "the substance" or "purport" of a users' interaction with the website. Thus, to the extent Cancelmo intends to assert a claim under the Disclosure Provision, he has adequately alleged that the defendants disclosed the contents of his communications.

Conclusion

For the foregoing reasons, the court grants the defendants' motion to dismiss (doc. no. 7) with respect to Count I without prejudice to Cancelmo's right to amend his complaint and denies the defendants' motion to dismiss with respect to Count II.

On or before October 30, 2025, Cancelmo shall file either an amended complaint or a notice that he does not intend to amend his complaint. The defendants are relieved of any obligation to answer or otherwise respond to the complaint pursuant to Federal Rule of Civil Procedure 12 until such time as Cancelmo has notified the court that he does not intend to file an amended complaint, in which case the defendants shall answer doc. no. 1-1 within 21 days of filing of such notification, or has filed an amended complaint, in which case the defendants shall answer or otherwise respond to the amended complaint within 21 days after filing of the amended complaint.

SO ORDERED.

Samantha D. Elliott
United States District Judge

September 30, 2025

cc: Counsel of Record