Lisota v. Heartland Dental, LLC et al Doc. 38

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

Megan Lisota,

Plaintiff,

v.

Heartland Dental, LLC *and* RingCentral, Inc.,

Defendants.

No. 25 CV 7518

Judge Lindsay C. Jenkins

MEMORANDUM OPINION AND ORDER

Heartland Dental, LLC ("Heartland") provides non-clinical services to dental clinics, like Tru Family Dental. As part of its services, it contracts with RingCentral, Inc. to provide an artificial intelligence-supported telephone service to its affiliates. Megan Lisota, a patient of Tru Family Dental, has sued both Heartland and RingCentral under the Federal Wiretap Act, alleging that RingCentral's product eavesdropped on and analyzed her calls to the clinic. Before the court are Defendants' motions to dismiss, which is partly granted.

I. Background[1]

Plaintiff Megan Lisota receives dental services from Tru Family Dental, a dental chain that outsources non-clinical functions—like administrative services and after-hour and overflow call center services—to Defendant Heartland. [Dkt. 1 ¶¶ 1, 5, 17, 20.] Heartland, meanwhile, contracts with Defendant RingCentral to provide cloud-based telephone services to affiliated practices. [*Id.* ¶ 2.] Specifically, "[a]s part of its DSO services, Heartland upgraded its dental partners' phones into one single system administered by RingCentral." [*Id.* ¶ 19.]

RingCentral's artificial intelligence software "capture[s] and transcribe[s] key details from patient, payer and provider calls in real-time," using "speech recognition and language learning models to turn conversations into live transcripts" and synopses. [*Id.* ¶¶ 12–15.] Heartland relies on these capabilities to identify and triage callers, and to identify missed opportunities to schedule appointments. [*Id.* ¶¶ 20–22.]

[1] The court accepts as true plaintiff's well-pleaded allegations and draws all reasonable inferences in her favor. *Thomas v. Neenah Joint Sch. Dist.*, 74 F.4th 521, 522 (7th Cir. 2023).

Dockets.Justia.com

Lisota, on several occasions over two years, called a Heartland-supported dental clinic, "identif[ying] herself by her name and inquir[ing] about making appointments to receive medical treatment." [*Id.* ¶ 31.] With no knowledge of—and having never consented to—RingCentral "eavesdropping and analyzing her calls," Lisota now raises a putative class action claim against Heartland and RingCentral for violating the Federal Wiretap Act. [*Id.* ¶¶ 32–34, 42–51.]

II. Legal Standard

A motion to dismiss pursuant to Rule 12(b)(1) challenges the court's subject-matter jurisdiction, while a motion to dismiss under Rule 12(b)(6) tests the legal sufficiency of the plaintiff's claims. In both cases, the court takes well-pleaded factual allegations as true and draws reasonable inferences in the plaintiff's favor. *Reardon v. Danley*, 74 F.4th 825, 827 (7th Cir. 2023); *Choice v. Kohn L. Firm, S.C.*, 77 F.4th 636, 638 (7th Cir. 2023). At the pleading stage, the court evaluates only whether the factual allegations "plausibly suggest" the existence of subject-matter jurisdiction under the familiar *Iqbal–Twombly* standard. *Silha v. ACT, Inc.*, 807 F.3d 169, 174 (7th Cir. 2015). *See also Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007); *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Then, to survive a motion to dismiss under Rule 12(b)(6), "a complaint's factual allegations 'must be enough to raise a right to relief above the speculative level.'" *Emerson v. Dart*, 109 F.4th 936, 941 (7th Cir. 2024) (quoting *Twombly*, 550 U.S. at 555 (2007)).

III. Analysis

Defendants argue that Lisota lacks standing to sue under the Federal Wiretap Act and that, in any event, statutory exceptions preclude liability. [Dkt. 24 at 1–2; Dkt. 25 at 5–6.[2]] Because her complaint alleges privacy harms analogous to the tort of intrusion upon seclusion, she has standing to pursue her claim. However, the Act's "ordinary course of business" exception is applicable, and so she fails to state a claim for relief.

A. Failure to Demonstrate Standing

Consistent with Article III's limitation of federal court jurisdiction to "cases and controversies," plaintiffs must have standing to pursue their cases. *Pucillo v. Nat'l Credit Sys., Inc.*, 66 F.4th 634, 637 (7th Cir. 2023). To establish standing, "the plaintiff must have suffered an injury in fact traceable to the defendant and capable of being redressed through a favorable judicial ruling." *Sweeney v. Raoul*, 990 F.3d 555, 559 (7th Cir. 2021) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992)). "The alleged injury must be 'concrete and particularized' as well as 'actual or imminent, not conjectural or hypothetical.'" *Id.* (quoting *Lujan*, 504 U.S. at 560).

[2] Citations to docket filings generally refer to the electronic pagination provided by CM/ECF, which may not be consistent with page numbers in the underlying documents.

Intangible injuries, like the apparent privacy invasions Lisota alleges, can be concrete, so long as they are "real, and not abstract." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016) (cleaned up). To this end, courts consider "whether the alleged injury to the plaintiff has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts." *TransUnion v. Ramirez*, 594 U.S. 413, 424 (2021) (quoting *Spokeo*, 578 U.S. at 341)). These include "four distinct [privacy] torts: intrusion upon seclusion, appropriation of another person's name or likeness, publicity given to another person's private life, and publicity that places one in a false light." *Nabozny v. Optio Sols. LLC*, 84 F.4th 731, 735 (7th Cir. 2023).

Beyond the general throughline of an invasion of privacy, Lisota's complaint does not clarify her theory of injury.[3] In the Seventh Circuit, generic analogies "to a tortious invasion of privacy" do not suffice to confer standing, but courts are permitted to look past "bare invasion-of-privacy allegation[s]" and consider "the relevant factual allegations" in the context of the four torts. *Id.* Here, Lisota's opposition brief touches on what this court agrees are the two most relevant analogies: (1) publicity given to another person's private life, and (2) intrusion upon seclusion. [*See* Dkt. 33 at 12 ("violations of the Federal Wiretap Act, particularly those involving unlawful access to or disclosure of protected medical information, constitute intrusions of an individual's private domain").] The latter is sufficient to confer standing.

First, one commits the common law tort of publicity, known also as the public disclosure of private facts, when "he 'gives publicity' to a matter that concerns 'the private life of another,' is 'highly offensive to a reasonable person,' and is not of legitimate public concern." *Nabozny*, 84 F.4th at 735 (quoting Restatement (Second) of Torts § 652D (A.L.I. 1977)). It requires either that the matter be communicated "to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge." *Id.* This is a qualitative—not quantitative—inquiry, and so "while the number of recipients might be a relevant consideration," more important is the character of the recipient and context of the disclosure. *Id.* (citing *Hunstein v. Preferred Collection & Mgmt. Servs., Inc.*, 48 F.4th 1236, 1246 (11th Cir. 2022)). For example, disclosure to a *single* journalist for publication promises more publicity than internal communication to *thousands* of confidentiality-bound employees. *See id.*

---

[3] As such, the parties' briefings fail to identify or debate what the court believes is the core standing inquiry—analogy to a specific common law tort. Lisota likens her situation to the Illinois Biometric Information Privacy Act, *see* Dkt. 33 at 11–12, but the Seventh Circuit has explained that the biometrics are uniquely immutable and personal, making comparison difficult. *See Nabozny*, 84 F.4th at 737. Meanwhile, Defendants argue primarily that Lisota fails to plead facts in a particularized fashion. [Dkt. 24 at 12; Dkt. 25 at 10.] However, it is reasonable to infer from her allegations that all calls to the clinic were intercepted in some form, including hers.

Nabozny and *Hunstein* are instructive as to why Heartland's "disclosure" does not implicate publicity. In *Nabozny*, the Seventh Circuit addressed a defendant's disclosure of private debt information to a third-party mail vendor, so the information could then be mailed to the plaintiff. 84 F.4th at 733. It held that this "transmission of information to a *single ministerial intermediary* [did] not remotely resemble the publicity element," and therefore, in a standing context, the alleged injury was insufficiently "analogous to the harm at the core of the public-disclosure tort." *Id.* at 736 (emphasis added). Meanwhile, in *Hunstein*, on which *Nabozny* relies, the Eleventh Circuit observed that the plaintiff "did not even allege that a single employee ever read or understood the information about his debt. Under even the most generous reading of his complaint, one company sent his information to another, where it was 'populated' into a private letter that was sent to his own home." 48 F.4th at 1248.

RingCentral is little more than a ministerial intermediary. Like a mail vendor, RingCentral provides a service that facilitates communication between individuals and entities already party to the correspondence. Lisota does not allege that it ever published, publicized, or otherwise shared any information—except, perhaps, in transcript form *back* to the call recipient(s). To the extent anything more is alleged of RingCentral, it's the company's use of call information to improve and develop its own products. But this is an entirely internal use, so there is no alleged risk that any information reaches the public, or else becomes public knowledge.

In this respect, Lisota's circumstances differ from cases involving invisible tracking pixels, in which a user's information is collected by third parties—like Meta and Google—precisely for marketing purposes, such as targeted advertising. *See Smith v. Loyola Univ. Med. Ctr.*, 2024 WL 3338941, at *4 (N.D. Ill. July 9, 2024); *A.M., et al. v. Adv. Reprod. Health Ctr., Ltd.*, No. 24 CV 7559, Dkt. 42 at 11–12 (N.D. Ill. Aug. 8, 2025); *L.C. v. Fertility Centers of Illinois, PLLC*, 2025 WL 3514494, at *5 (N.D. Ill. Dec. 8, 2025). As the Second Circuit explained in contrasting pixel tracking with *Nabozny*'s mail vendor, companies like Meta (1) are permitted to "sell, disclose, or otherwise use [the] data for additional purposes," (2) cross-reference the data with their own digital profiles, (3) do not collect data to then "bounce [it] back" but rather harness it "for its own commercial purposes, not the [client's] or the user's," and (4) use it for digital advertising, "an industry that "underlies many of the Internet's most widely used services." *Salazar v. Nat'l Basketball Ass'n*, 118 F.4th 533, 543 (2d Cir. 2024) (internal citations omitted). RingCentral's uses are decidedly different, neither inviting nor risking anything comparable to "public scrutiny." *Nabozny*, 84 F.4th at 736. For that reason, analogy to the tort is insufficient to confer standing.

More apt, then, is the tort of intrusion upon seclusion, "which occurs when a person intrudes upon the solitude or seclusion of another or his private affairs or concerns, and this intrusion would be highly offensive to a reasonable person." *Persinger v. Sw. Credit Sys., L.P.*, 20 F.4th 1184, 1192 (7th Cir. 2021) (cleaned up).

"Eavesdropping by wiretapping is a quintessential example of this, *see Ramirez v. LexisNexis Risk Sols.*, 729 F. Supp. 3d 838, 850 (N.D. Ill. 2024), and precisely the kind of injury that Lisota alleges here. [*See, e.g.*, Dkt 1 ¶¶ 30, 44.]

Indeed, in identifying analogies for standing purposes, courts are "meant to look for a 'close relationship' in kind, not degree." *Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458, 462 (7th Cir. 2020). "Whether [she] would prevail in a lawsuit for common law invasion of privacy is irrelevant. It is enough to say that the harm alleged in her complaint resembles the harm associated with intrusion upon seclusion." *Persinger*, 20 F.4th at 1192. Disregarding the intrusion-upon-seclusion analogy would require this court to wade too far into the merits, and to reject her plausible framing of RingCentral as an "unannounced listener and auditor of patients' phone calls." [Dkt. 1 ¶ 23.]

Therefore, though neither the complaint nor Lisota's opposition brief spells it out in exact terms, her injury sufficiently resembles the tort of intrusion upon seclusion to survive Defendants' collective challenge.

B. Failure to State a Claim under the Wiretap Act

Lisota argues that, "[b]y partnering with RingCentral to eavesdrop on … telephone conversations in real-time, Defendant Heartland allowed Defendant RingCentral to intercept, or procured RingCentral to intercept, the content of wire and/or oral communications." [Dkt. 1 ¶ 44.] Therefore, she says, both companies violated the Federal Wiretap Act—RingCentral as the eavesdropper, and Heartland as the facilitator. Defendants, however, argue that the statute exempts them from liability.

The Act "imposes civil liability on anyone who 'intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication.'" *In re TikTok, Inc. In-App Browser Priv. Litig.*, 2024 WL 4367849, at *9 (N.D. Ill. Oct. 1, 2024) (citing 18 U.S.C. §§ 2511(1)(a), 2520(a)). Critically, the Act excepts interceptions "by a provider of wire or electronic communication service in the ordinary course of its business," § 2510(5)(a)(ii), as well as those by "a party to the communication or where one of the parties to the communication has given prior consent to such interception," unless done "for the purpose of committing any criminal or tortious act." § 2511(2)(d). Defendants raise both exceptions, and the court finds the first clearly applicable.[4]

[4] Lisota argues that "these exemptions are affirmative defenses" that she need not plead around. [Dkt. 33 at 22.] The court, however, considers them based on her complaint's own allegations, as courts routinely do. *See, e.g.*, *Matera*, 2016 WL 8200619, at *14.

a. Ordinary Course of Business Exception

"Intercept," as defined in the Act, contemplates the "use of any electronic, mechanical, or other device"—though not those "used by a provider of wire or electronic communication service in the ordinary course of its business." § 2510. Lisota does not dispute that RingCentral is an electronic communication service, describing it as "an Internet-based telephone provider" comparable to "a traditional telephone provider." [Dkt. 1 ¶ 11.] Rather, she challenges whether the interception occurred in the ordinary course of business. [*See* Dkt. 33 at 23.]

To construe "ordinary course of business," courts apply one of two tests. One, which Lisota endorses, requires "some nexus between the need to engage in the alleged interception and the [provider's] ultimate business, that is, the ability to provide the underlying service or good." *In re TikTok*, 2024 WL 4367849, at *13 (quoting *Matera v. Google Inc.*, 2016 WL 8200619, at *9 (N.D. Cal. Aug. 12, 2016)). The other, which Defendants prefer, "extends the exception to any actions taken in furtherance of a provider's 'legitimate business purposes.'" *Id.* (quoting *In re Google, Inc. Priv. Pol'y Litig.*, 2013 WL 6248499, at *11 (N.D. Cal. Dec. 3, 2013)).

This court need not favor either to conclude that the exception applies. Even under Lisota's more narrow approach, the complaint establishes a nexus between the interception's necessity and the services RingCentral provides. Put differently, the interception "facilitate[s] the provision of [call] services" or is "incidental" to providing them. *Matera*, 2016 WL 8200619, at *14.

Lisota disagrees. In her response brief, she argues that "the use of AI-analysis and training is entirely unnecessary to facilitate the making and receiving of calls or messages between dental practices and their patients." [Dkt. 33 at 23.] But RingCentral's business, as advertised to customers, is not simply to "facilitate the making and receiving of calls or messages"—at least not as framed in the complaint.

As Lisota pleads, RingCentral explicitly offers businesses a product that "power[s] every interaction with AI that integrates seamlessly across your calls, messages, meetings, and contact center," and it emphasizes its ability to provide "real-time insights, and create effortless workflows." [Dkt. 1 ¶ 12.] The complaint highlights key features, including "(i) real-time voice transcription, (ii) call highlights, (iii) automated call summaries and (iv) sentiment voice analysis." [*Id.* ¶ 13.] These features "provide concise and easy to understand AI-generated synopsis of calls" and allow customers to "see AI-generated key phrases, next steps, and follow-up items." [*Id.* ¶ 15.] So, too, does RingCentral analyze tone to help businesses "understand a person's emotional state during a conversation." [*Id.* ¶ 16.]

Indeed, RingCentral explicitly bills its phone system as an "AI-powered business communications platform." [*Id.* ¶ 19.] That it does more than simply facilitate the making and receiving of calls is therefore critical to its pitch. [*See id.*

¶ 14 ("Real-time AI transcription lets you focus on the conversation at hand, not taking notes.")] Necessary, then, is its ability to "listen and analyze" calls in real-time—what Lisota elsewhere describes as "eavesdropping." [*Id.* ¶¶ 22, 32–34.] In other words, it cannot facilitate its core service without real-time listening, transcription, and analysis.

This distinguishes its situation from the services and interceptions in Lisota's preferred authorities, all of which involve targeted advertising informed by the content of intercepted emails and direct messages. *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 844 (N.D. Cal. 2014) (finding no "nexus between Facebook's alleged scanning of users' private messages for advertising purposes and its ability to provide its service"); *In re Google Inc.*, 2013 WL 5423918, at *11 (N.D. Cal. Sept. 26, 2013) (same, emphasizing allegation that Google used intercepted email content "for its own benefit in other Google services unrelated to the service of email or the particular user"); *Matera*, 2016 WL 8200619, at *14 (same, emphasizing allegation that "Google 'intercepts Gmail for the distinct purpose of acquiring and retaining user data and creating targeted advertising,' which is separate from 'the functioning of the provided communication service'").

Lisota does identify two "separate business objectives" that she argues, in her brief, are "wholly unrelated to providing telecommunications services." [Dkt. 33 at 23.] First, "the use of artificial intelligence to generate more appointments for supported practices," and second, use of "customer calls to refine AI algorithms across RingCentral's various, distinct, products and services for other customers." [*Id.*] The first, however, is an example of how RingCentral actually integrates listening and analysis into its phone service. [*See* Dkt. 1 ¶ 22 (quoting a Heartland executive's description of how AI flags appointment opportunities for "an outbound call queue for our agents, who typically respond back to the patient within 10 minutes.")] In any event, this objective—"to generate more appointments"—is Heartland's, not RingCentral's.

Meanwhile, the second objective—training algorithms with call data—is, at minimum, "incidental to the provision of [RingCentral's] electronic communication service." *Matera*, 2016 WL 8200619, at *14. As the complaint alleges, RingCentral processes user data for purposes that "include providing, monitoring, supporting, improving, and maintaining the Services." [Dkt. 1 ¶ 28.] The closest that the defendants in Lisota's authorities come to arguing something similar is that "the alleged interception of email enables Google to provide targeted advertising, which in turn generates the revenue necessary for Google to provide Gmail." *Matera*, 2016 WL 8200619, at *14. But funding a service, since money is fungible, is more clearly separate than directly maintaining and improving one. Absent plausible allegations that RingCentral processed call data for reasons distinct from its communication service, Lisota's protests fall flat.

Therefore, because RingCentral's "interception" fits within the "ordinary course of business" exception, it is not an interception as defined by the statue. Consequently, it is not liable under the Act, nor is Heartland liable for procuring it.

b. Party Exception

Parties to the communication, and those to whom they consent, are similarly exempt from liability. § 2511(2)(d). "Courts are clear that in the context of the Wiretap Act, 'a party to the conversation is one who takes part in the conversation.'" *Zak v. Bose Corp.*, 2019 WL 1437909, at *3 (N.D. Ill. Mar. 31, 2019) (collecting cases). The inquiry is "relatively simple for telephone calls," with a single line of communication between two persons. *In re TikTok*, 2024 WL 4367849, at *11 (citing *United States v. Pasha*, 332 F.2d 193, 198 (7th Cir. 1964)).

Lisota identifies a wrinkle, though. "She intended to call her dental provider, Tru Family Dental," not its DSO, Heartland. [Dkt. 33 at 14.] Unlike cases that "concern interceptions that were only one step removed from the intended party to the communication," her situation involves two layers of disclosure. [*Id.* at 16 ("Plaintiff alleges that she called Tru Family Dental, who disclosed the calls to Heartland, who disclosed them to RingCentral"). Therefore, she argues, Heartland was not a party—and any "consent was not Heartland's to give." [*Id.*]

It's unclear as to who, precisely, answered Lisota's calls—Tru Family Dental or Heartland. Lisota alleges that she *intended* to call the former, *see* Dkt. 1 ¶ 31, but the complaint, as written, leaves open two possibilities as to who was on the other end. It alleges that Heartland "provides after hour and overflow call center services to its partner dental practices," and that it "automatically routes certain calls … to a Heartland Patient Service team depending on the local clinic's availability," but also that it lets existing patient calls "ring a few more times at the practice before [it] grab[s] them, because [it] want[s] to give the local staff a chance to have those conversations and build those relationships." [*Id.* ¶¶ 20–21.] It is therefore plausible that when Lisota called, either Tru Family Dental staff *or* Heartland answered.

If Heartland participated directly, the analysis is simple. As it argues, its direct "participation in the calls, even if unintended by Plaintiff, renders it not liable under the Wiretap Act." [Dkt. 35 at 9.] "Indeed, a defendant is a 'party' to the communication within the meaning of the Wiretap Act when the defendant is a participant, even if the defendant was not an *intended* participant." *Zak*, 2019 WL 1437909, at *3 (citing *United States v. Pasha*, 332 F.2d 193, 198 (7th Cir. 1964)). The Seventh Circuit held so explicitly in *Pasha*, and Congress "specifically mentioned *Pasha* in its discussions of the 'party to the communication' provision" when amending the Act to its current state. *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 144 (3d Cir. 2015). Therefore, if Heartland answered Lisota's call, it was a party to the

communication as contemplated by the Act and, as such, within its rights to consent to RingCentral's "interception." Neither party would then be liable.[5]

The second scenario is more complex. If Tru Family Dental's local staff answered, the 'party exception' argument holds only if Tru Family Dental consented (or if Heartland was otherwise a party to the call).

Lisota argues that "Defendants have not even attempted to establish that Plaintiff or her dental provider consented to the interception at issue here, nor could they, given the allegations in the complaint." [Dkt. 33 at 16.] Nor, she says, did Heartland necessarily consent on Tru Family Dental's behalf. [*See id.* at 16–17.] True, nobody alleges or argues that Tru Family Dental expressly consented to RingCentral's access. Rather, as RingCentral responds, the "dental office contracted with Heartland, who in turn contracted with RingCentral, specifically to receive the services that Plaintiff now challenges." [Dkt. 34 at 8 (cleaned up).]

This, then, touches on matters of agency and authority that neither party briefed. Because the "ordinary course of business" exception more cleanly disposes of Lisota's claim, the court declines to itself pull the thread.[6]

IV. Conclusion

For these reasons, the court grants Defendants' motions to dismiss for failure to state a claim but the dismissal is without prejudice.

Enter: 25-cv-7518
Date: January 13, 2026

Lindsay C. Jenkins

[5] In response to Defendants' motions, Lisota mentions "Heartland's interception," seemingly implying that Heartland also violated the Act as an eavesdropper—not simply by procuring RingCentral's interception. [Dkt. 33 at 16.] But the complaint frames Heartland only in the latter role. Regardless, Lisota pleads no facts that show Heartland could have intercepted her information *unless* it was party to the call (and thus excepted from liability).

[6] RingCentral also argues that *it*, as a technology provider that facilitated the call, was party to the communication—an argument courts are split in resolving. *Compare In re TikTok*, 2024 WL 4367849, at *13 (rejecting argument where "defendant here is not the website operator (using the telephone analogy, the person on the other end of the phone line), but the browser operator (i.e., the phone company)"), *with Licea v. Am. Eagle Outfitters, Inc.*, 659 F. Supp. 3d 1072, 1083 (C.D. Cal. 2023) (holding that "third party [vendor, like Salesforce or Webex] was not an eavesdropper where their software collected clients' data, kept the data on its servers, and allowed clients to analyze their data"). Again, because the party exception is not necessary to resolve the claim against RingCentral, the court declines to endorse either approach at this time.