UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

W.W.,

Plaintiff,

v. Case No: 6:24-cv-1068-JSS-RMN

ORLANDO HEALTH, INC.,

Defendant.
_____/

ORDER

Defendant moves to dismiss Plaintiff's complaint for failure to state a claim. (Dkt. 17.) Plaintiff opposes the motion. (Dkt. 20.) Upon consideration, for the reasons outlined below, the motion is granted in part and denied in part.

BACKGROUND[1]

Defendant is a healthcare organization that operates over one hundred medical facilities throughout Florida and maintains a website at www.orlandohealth.com,[2] "which [Defendant] encourages patients to use for booking medical appointments, locating specific physicians and treatment facilities, [and] communicating medical

[1] The court accepts the well-pleaded factual allegations in the complaint as true and construes them in the light most favorable to Plaintiff. *See Harry v. Marchant*, 291 F.3d 767, 769 (11th Cir. 2002) (en banc).

[2] It is unclear from Defendant's motion whether it requests the court take judicial notice of its website. (*See* Dkt. 17 at 4 n.2.) But Defendant does not cite or meet the standard for taking judicial notice. (*See id.*) *See* Fed. R. Evid. 201(b)(2). As a result, the court does not judicially notice Defendant's website. *See Lodge v. Kondaur Cap. Corp.*, 750 F.3d 1263, 1273 (11th Cir. 2014) (stating that "the taking of judicial notice of facts is a highly limited process" because it "bypasses the safeguards which are involved with the usual process of proving facts by competent evidence" (quotation omitted)).

symptoms, conditions, and treatments via the search bar and related webpages." (Dkt. 1 at 2, 7–8.) Defendant's patients can also use its website to access the MyChart Patient Portal, through which they can schedule medical appointments, review their medical records, pay bills, communicate with their providers, order prescription refills, and complete forms. (*Id.* at 2.) Plaintiff is one of Defendant's patients. (*Id.* at 34.)

Allegedly, without informing its patients, Defendant "installed tracking technologies . . . onto its [w]ebsite." (*Id.* at 2.) These technologies include tools developed by Meta, Facebook's parent company, Google, and other social media companies. (*Id.* at 3.) Plaintiff alleges that the tools can be used to "gather, identify, target, and market products and services to Defendant's patients" and to "intercept, record, and disseminate patients' communications with Defendant." (*Id.* at 3, 15.) According to Plaintiff, Meta and Google offer these tracking tools "as software that advertisers can integrate into their webpages, . . . thereby enabling the interception and collection of user communications and activity on those platforms." (*Id.* at 15.) Essentially, in Plaintiff's view, these tools intercept and transmit users' "communications with the host webpage," Defendant's website, to a third party like Meta or Google. (*Id.* at 16.) Plaintiff explains: "For example, the Facebook Pixel on Defendant's [w]ebsite causes the user's web browser to instantaneously duplicate the contents of the communication with the [w]ebsite and send the duplicate from the user's browser directly to Facebook's server." (*Id.*) Plaintiff describes this software as hidden from users' view and difficult to avoid, even for the "particularly tech-savvy user." (*Id.* at 13–14, 17; *see id.* at 17 (discussing the "Conversions Application

Programming Interface," or CAPI, which "functions as a redundant measure to circumvent any ad blockers or other denials of consent by the website user").) Because of these tracking tools, Plaintiff claims, Meta and Google gained access to information regarding her status as a medical patient, her health conditions, her desired treatment, and her preferred physician or specialist, as well as any information included in phrases and search queries she entered into Defendant's website. (*Id.* at 19.) Moreover, because information was attached to her Facebook and Google identifiers, those third parties were allegedly able to associate the specific information entered into Defendant's website with Plaintiff's identity. (*Id.* at 19–20.) In exchange for providing access to user information, hosts like Defendant obtain "enhanced advertising services and more cost-efficient marketing" on social media platforms. (*Id.* at 47–48.)

Plaintiff brings this complaint on behalf of herself and others similarly situated. (*Id.* at 51.) She has used Defendant's website and its MyChart Patient Portal "to communicate [p]rivate [i]nformation to Defendant on numerous occasions to receive healthcare services from Defendant or [its] affiliates." (*Id.* at 34.) Specifically, Plaintiff used Defendant's website to identify gastroenterologists and cardiologists for treatment of her ileostomy, heart pains, fatty liver disease, and other ailments. (*Id.* at 35.) In seeking this treatment, Plaintiff used "Defendant's [w]ebsite and/or MyChart Patient Portal" to complete forms to book medical appointments, authorize treatments, and request medical records and invoices, to communicate with providers, and to conduct general research regarding her symptoms and possible treatment options. (*Id.* at 34–35.) While Plaintiff "never consented to the use of her [p]rivate

[i]nformation by [u]nauthorized [p]arties or to Defendant enabling [u]nauthorized [p]arties to access or interpret such information," she reports that after using Defendant's website, she "observed advertisements on her Facebook account for ileostomy bags, products or services related to strokes, aortic stenosis, and heart failure, neuropathy doctors from Orlando Health, and spinal decompression." (*Id.* at 37–38.) Citing the tracking tools and the advertisements she received for products and services related to her medical conditions, Plaintiff alleges that Defendant unlawfully shared her protected health information and private information with unauthorized third parties. (*Id.*)[3]

Plaintiff alleges that Defendant shared her private information with Meta and Google, among other companies, and that this data sharing constitutes a breach of her privacy and violates state and federal law. (*Id.* at 38–39.) Accordingly, Plaintiff brings six claims against Defendant: violation of the Florida Security of Communications Act (FSCA), Fla. Stat. § 934.01 (Count I), violation of the Wiretap Act as amended by the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2511(1) (Count II), breach of confidence (Count III), invasion of privacy—intrusion upon seclusion (Count IV), unjust enrichment (Count V), and breach of implied contract (Count VI).

[3] In this context, "[p]rotected health information [generally] means individually identifiable health information . . . that is . . . [t]ransmitted by electronic media . . . or . . . in any other . . . medium." 45 C.F.R. § 160.103. "Individually identifiable health information," in turn, includes "any information" that is "received by a health[]care provider" and "[r]elates 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," provided the information "identifies the individual" or "there is a reasonable basis to believe the information can be used to identify the individual." *Id.*

(Dkt. 1 at 57–72.) As relief, Plaintiff seeks compensatory, statutory, punitive, and nominal damages, legal fees, and an injunction to prevent Defendant from disclosing its patients' private information. (*Id.* at 72–73.)

APPLICABLE STANDARDS

Federal Rule of Civil Procedure 8 requires a complaint to include a "short and plain statement of [a] claim showing that the [plaintiff] is entitled to relief." Fed. R. Civ. P. 8(a)(2). "[T]he pleading standard Rule 8 announces does not require 'detailed factual allegations,' but it demands more than an unadorned, the-defendant-unlawfully-harmed-me accusation." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007)). "Rule 8 marks a notable and generous departure from the hypertechnical, code-pleading regime of a prior era, but it does not unlock the doors of discovery for a plaintiff armed with nothing more than conclusions." *Id.* at 678–79.

In deciding a motion to dismiss a complaint for failure to state a claim, a court "accept[s] the allegations in the complaint as true and construe[s] them in the light most favorable to the plaintiff." *Henley v. Payne*, 945 F.3d 1320, 1326 (11th Cir. 2019). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 570). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.*

ANALYSIS

Defendant moves to dismiss each of Plaintiff's claims. (Dkt. 17 at 8–25.) The court addresses its arguments as to each claim in turn.

A. Violation of the FSCA

The FSCA prohibits "[i]ntentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept any . . . electronic communication." Fla. Stat. § 934.03(1)(a). It defines "intercept" as "the aural or other acquisition of the contents of any . . . electronic . . . communication through the use of any electronic, mechanical, or other device." Fla. Stat. § 934.02(3). It further defines "contents" as "any information concerning the substance, purport, or meaning of that communication." Fla. Stat. § 934.02(7). Because the FSCA was modeled after the Wiretap Act, Florida courts construe the FSCA's provisions in accord with the meaning given to analogous provisions of the Wiretap Act. *See Minotty v. Baudo*, 42 So. 3d 824, 831 (Fla. Dist. Ct. App. 2010) ("[The FSCA] was modeled after the [f]ederal Wiretap Act . . . . Florida follows federal courts as to the meaning of provisions after which [the FSCA] was modeled."). "The touchstone in many cases arising under the FSCA . . . is th[e] definition of *contents*." *Goldstein v. Costco Wholesale Corp.*, 559 F. Supp. 3d 1318, 1321 (S.D. Fla. 2021).

This case is no exception. Defendant argues that Plaintiff's FSCA claim must be dismissed because Plaintiff fails to allege that the "contents" of any of her communications were intercepted. (*See* Dkt. 17 at 9–12.) Defendant relies principally on a Florida state court case, *Jacome v. Spirit Airlines, Inc.*, No. 2021-000947-CA-01,

2021 WL 3087860 (Fla. Cir. Ct. June 17, 2021). That court was considering allegations that the defendant "utilized at least one session replay script"—software that "tracks a website browser's movements"—"to contemporaneously intercept the substance of [the p]laintiff's electronic communications with [the d]efendant's website, including mouse clicks and movements, keystrokes, search terms, information inputted by [the p]laintiff, and pages and content viewed by [the p]laintiff." *Id.* at *1. The court found that the use of session replay software was not covered by the FSCA. *See id.* at *2. The court also determined that the FSCA claim was due to be dismissed as the information at issue was not "contents" as defined by the FSCA, because the plaintiff's "mouse clicks and movements, keystrokes, search terms, information inputted . . . , and pages and content viewed" did "not convey the *substance* or *meaning* of any message." *Id.* at *4. Several federal district courts have since applied the reasoning of *Jacome* in cases that also alleged a violation of the FSCA based on the use of session replay technology on commercial websites. *See, e.g.*, *Cardoso v. Whirlpool Corp.*, No. 21-CV-60784-WPD, 2021 WL 2820822 (S.D. Fla. July 6, 2021).

Here, *Jacome* supports denying Defendant's motion to dismiss. It does so in three ways. First, the *Jacome* court addressed a different technology, session replay, employed in a generic commercial setting, when it dismissed the FSCA claim. *See Jacome*, 2021 WL 3087860, at *1. The court determined that the FSCA's definition of "electronic communication," which "exclude[s] '[a]ny communication from an electronic or mechanical device which permits the tracking of the movement of a

person or an object,'" did not apply to session replay technology, "which *tracks* a website browser's movements." *Id.* at *3 (quoting § 934.02(12)(c) (excluding from the definition of "[e]lectronic communication" "[a]ny communication from an electronic . . . device which permits the tracking of the movement of a person or an object")). Defendant's argument that the difference in technology is of no moment, (*see* Dkt. 17 at 10 n.5), is not persuasive because Plaintiff's claims are predicated on the tracking tools' interception of her communications, (*see, e.g.*, Dkt. 1 at 59), not on the simple fact that her movements on Defendant's website were tracked. *See Jacome*, 2021 WL 3087860, at *3 ("Here, [the p]laintiff seeks to hold [the defendant] liable for its use of session replay software which *tracks* a website browser's movements.").

Other district courts considering factually closer cases—involving the same tracking tools at issue here utilized on healthcare providers' websites—have reached the opposite conclusion as the *Jacome* court. The Northern District of Illinois, for example, in a case involving the same tracking tools as those used by Defendant, denied a motion to dismiss the plaintiffs' FSCA claim. *See A.D. v. Aspen Dental Mgmt., Inc.*, No. 24 C 1404, 2024 WL 4119153, at *5–7 (N.D. Ill. Sept. 9, 2024) (finding allegations that URLs "included [the p]laintiffs' search terms about medical conditions and types of treatments" "sufficient to plausibly allege that covered 'content' was intercepted"). Similarly, the Central District of California in *R.C. v. Walgreen Co.* denied a motion to dismiss claims brought under the Wiretap Act and California's

analogous state statute, the California Invasion of Privacy Act (CIPA),[4] based on allegations that the defendant had permitted tracking technologies, including the Meta Pixel, to be used on its website. 733 F. Supp. 3d 876, 885, 903 (C.D. Cal. 2024). These technologies shared with Meta and Google the contents of the website users' communications, which included names of "sensitive healthcare products" that the users were searching on the defendant's website. *Id.* at 885–86. This data sharing resulted in those users, much like Plaintiff here, "receiving targeted ads on their Facebook accounts related to the medical conditions and treatments they disclosed to [the d]efendant." *Id.* at 886. Because the information provided to Meta and Google "reveal[ed] a substantive message about [the p]laintiffs' health concerns," the court determined that the information constituted "contents" under the Wiretap Act and the CIPA. *Id.* at 902; *accord In re Grp. Health Plan Litig.*, 709 F. Supp. 3d 707, 712, 718, 720 (D. Minn. 2023) (determining that the defendant's use of technology to "surreptitiously track[] users' interactions on the [defendant's w]ebsites and transmit[] those interactions to [Meta]" was actionable under the Wiretap Act and that "a URL that discloses a search term or similar communication made by the user can be considered a communication under the statute" (quotation omitted)); *Doe v. Microsoft Corp.*, No. C23-0718-JCC, 2023 WL 8780879, at *9 (W.D. Wash. Dec. 19, 2023) ("[The p]laintiff alleges [the defendant] collects URLs containing search queries that could divulge a user's medical conditions, allergies, and immunizations. Accordingly,

[4] As with the FSCA, "[t]he analysis for a violation of [the] CIPA is the same as that under the federal Wiretap Act." *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020) (quotation omitted).

[the p]laintiff has adequately pled that [the defendant] intercepted the contents of her communication with [a healthcare provider] for purposes of [the] CIPA." (citation omitted)).

Second, *Jacome* supports denying Defendant's motion to dismiss the FSCA claim because in concluding that the plaintiff had not adequately alleged that the "contents" of an electronic communication had been intercepted, the *Jacome* court relied primarily on *In re Zynga Privacy Litigation*, 750 F.3d 1098 (9th Cir. 2014), which the court found "instructive." *Jacome*, 2021 WL 3087860, at *3. The *In re Zynga* court concluded that the "refer[r]er header information at issue," which "include[d] only basic identification and address information," did not qualify as "contents" under the Wiretap Act. 750 F.3d at 1109. However, in reaching that conclusion, the Ninth Circuit stated that circumstances such as those alleged by Plaintiff here *could* constitute a violation of the Wiretap Act. *Id.* at 1108–09 ("Under some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging a URL containing that search term to a third party could amount to disclosure of the contents of a communication."). Accordingly, courts considering allegations such as Plaintiff's generally find that *In re Zynga* supports the claims. *See, e.g.*, *Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1076 (N.D. Cal. 2023) ("And while a URL that includes 'basic identification and address information' is not 'content,' a URL disclosing a 'search term or similar communication made by the user' 'could constitute a communication' under the [Wiretap Act]." (quoting *In re Zynga*, 750 F.3d at 1108–09)).

Third, in determining that the FSCA did not apply to session replay technology, the *Jacome* court looked to the intent of the Florida and federal legislatures in passing the FSCA and the Wiretap Act. 2021 WL 3087860, at *3. That court concluded that these bodies did not intend either act to "extend to the use of commonplace analytics software to improve a website browser['s] experience." *Id.* However, in reaching that conclusion, the *Jacome* court specifically noted that the FSCA was designed to protect precisely the information at issue in this case—private medical information. *See id.* at *2 ("[T]he [c]ourt agrees with [the defendant] that Congress's main concern in amending the [f]ederal Wiretap Act to include electronic communications (which prompted the Florida legislature to likewise amend the FSCA) was to protect private personal and business records (like medical records) from interception on computerized recordkeeping systems." (footnote omitted)).

For these reasons, Defendant's reliance on *Jacome* is misplaced, and Plaintiff has adequately alleged that the electronic communications she claims were intercepted were "contents" as defined by the FSCA. *See R.C.*, 733 F. Supp. 3d at 902–03 (concluding that because "[the p]laintiffs allege[d] that the data collected by [the d]efendant and transmitted to third parties include[d] personal health information" and that "such information reveal[ed] a substantive message about [the p]laintiffs' health concerns," the "[p]laintiffs ha[d] adequately alleged contents"). Indeed, this conclusion is supported by the definition of "contents." The FSCA's current definition of "contents" has been substantively unchanged since its passage in 1969. *Compare* Fla. Stat. § 934.02(7) (2024) ("'Contents,' when used with respect to any wire, oral, or

electronic communication, includes any information concerning the substance, purport, or meaning of that communication."), *with* Fla. Stat. § 934.02(7) (1969) ("'Contents,' when used with respect to any wire or oral communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication."). This language is identical to the definition of "contents" originally included in the Wiretap Act. *See* 82 Stat. 213 (1968). The key words here are "substance," "purport," and "meaning." "A fundamental canon of statutory construction is that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning." *Perrin v. United States*, 444 U.S. 37, 42 (1979). "When examining the plain and ordinary meaning of a statute, one of the ways to figure out that meaning is by looking at dictionaries in existence around the time of enactment." *United States v. Chinchilla*, 987 F.3d 1303, 1308 (11th Cir. 2021) (quotation omitted).

A dictionary from the relevant period defines "substance" to mean "[e]ssence; the material or essential part of a thing," "purport" to refer to "[m]eaning; import; substantial meaning; substance," and "meaning" to refer to "[t]hat which is, or is intended to be, signified or denoted by act or language." *Substance*, *Purport*, *Meaning*, Black's Law Dictionary (4th ed. 1968); *see In re Zynga*, 750 F.3d at 1106 (looking to the analogous provision of the Wiretap Act and determining that "substance" means "the characteristic and essential part," "purport" means the "meaning conveyed, professed or implied," and "meaning" refers to "the thing one intends to convey . . . by language" (quoting Webster's Third New International Dictionary 2279 (1981)). The

information at issue here is the message Plaintiff sought to convey to Defendant through its website—information related to her medical conditions and providers—and thus constitutes the substance, purport, or meaning of her communications. (*See* Dkt. 1 at 59.)

In addition to discussing *Jacome* and its progeny, Defendant argues that Plaintiff "fails to allege facts showing that the substantive contents of any of her communications on [Defendant's w]ebsite were unlawfully intercepted by [Defendant]." (Dkt. 17 at 11 (citation and emphasis omitted).) Specifically, Defendant asserts that Plaintiff "crafts her allegations in a way to suggest that her information inputted on [Defendant's w]ebsite may have been intercepted, but falls short of alleging whether there was an interception and, more importantly, what precisely was plausibly 'intercepted.'" (*Id.* (emphasis omitted).) In her complaint, however, Plaintiff alleges that Defendant permitted unauthorized parties to intercept her "internet communications while accessing [Defendant's website], including the contents thereof," which encompassed "the URL visited, the medical conditions and types of doctors searched," and other medical information related to her. (Dkt. 1 at 59.) This allegation is in addition to the myriad of factual details Plaintiff provides that are specific to Defendant's website regarding how these communications are intercepted and what information is intercepted, (*id.* at 21–34), as well as her allegations that after inputting information regarding her illnesses onto Defendant's website, she received advertisements from Meta related to those same illnesses, (*id.* at 34–39). Accepting these allegations as true and construing them in the light most

favorable to Plaintiff, the court finds that they are sufficient to state a plausible claim for relief. *See Henley*, 945 F.3d at 1326.

The court is also persuaded by the analysis of the Northern District of Florida, which was considering a case essentially on all fours with this one. That court provided the following summary of its case:

> [The defendant] is a healthcare system that operates Tallahassee Memorial Hospital [(TMH)]. In addition to the physical hospital, TMH owns and operates the website https://www.tmh.org. [The p]laintiff is a TMH patient who . . . used TMH's website to communicate information about her health on the condition that it would be kept confidential and not disclosed to any unauthorized third parties. However, [the p]laintiff alleges that unbeknownst to her, TMH installed software on its public website that tracked her movements and searches. [The p]laintiff further alleges that through this software, TMH disclosed [the p]laintiff's private information to third parties—specifically, Google and Meta.

D.S. v. Tallahassee Mem'l HealthCare, No. 4:23cv540-MW/MAF, 2024 WL 2318621, at *1 (N.D. Fla. May 22, 2024) (quotation omitted). The court determined that the plaintiff's allegations were sufficient to overcome the defendant's motion to dismiss the plaintiff's claims, which included FSCA and Wiretap Act claims in addition to claims of breach of confidence, invasion of privacy, unjust enrichment, and breach of implied contract. *Id.* "[R]esolution of these claims," that court reasoned, "involves answering highly technical questions[, including] . . . whether and to what extent the contents of [the p]laintiff's activities can be considered 'communications' for purposes of the FSCA . . . . This [c]ourt declines to make dispositive merits determinations on

a motion to dismiss, where the Rule 8 bar is low." *Id.* *See also Cyr v. Orlando Health, Inc.*, No. 8:23-cv-588-WFJ-CPT (M.D. Fla. July 5, 2023), Dkt. 37 (denying motion to dismiss highly similar complaint against Defendant after a hearing, finding that "[t]he assertions set forth by [the p]laintiff are plausible, thus entitling them at this stage to being considered true as alleged" and noting that "[t]he [c]ourt f[ound] little utility in a pleadings repartee at the beginning of a case" so "complicated and well-lawyered").[5]

Because Plaintiff has plausibly alleged a claim under the FSCA, Defendant's motion to dismiss that claim is denied.

B. Violation of the Wiretap Act

The Wiretap Act generally prohibits the unauthorized interception of electronic communications and the intentional disclosure or use of the contents of an intercepted communication. 18 U.S.C. § 2511(1)(a), (c), (d). Because FSCA claims are analyzed in the same manner as claims brought under the Wiretap Act, Defendant reasserts the arguments it made as to Plaintiff's FSCA claim, (Dkt. 17 at 12), and the court finds those arguments unavailing for the reasons discussed above. The only independent argument raised by Defendant for the dismissal of the Wiretap Act claim is that as a party to the communications at issue, Defendant cannot have unlawfully intercepted those communications. *See* 18 U.S.C. § 2511(2)(d) ("It shall not be unlawful under this chapter for a person not acting under color of law to intercept a[n] . . . electronic

[5] The parties note that the instant case is related to *Cyr*. (*See* Dkt. 17 at 3 & n.1; Dkt. 20 at 2.) After surviving Defendant's motion to dismiss her complaint, the plaintiff in *Cyr* sought leave to amend her complaint to add Plaintiff as a party, which request was denied as untimely. *Cyr*, No. 8:23-cv-588-WFJ-CPT (M.D. Fla. Feb. 13, 2024), Dkt. 53.

communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception . . . ."); *Ramos v. Delphi Behav. Health Grp., LLC*, No. 21-11218, 2022 WL 1415856, at *1 (11th Cir. May 4, 2022) ("[I]t is lawful for an individual to intercept a communication if he is a party to it."). Plaintiff argues that her Wiretap Act claim is not barred in light of the crime-tort exception to this rule, under which a party to the communication may be liable if the "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any [s]tate." 18 U.S.C. § 2511(2)(d). The parties agree that Plaintiff's Wiretap Act claim hinges upon whether or not this crime-tort exception applies. (*See* Dkt. 17 at 12–16; Dkt. 20 at 7–12.)

Plaintiff alleges that Defendant "intentionally intercepted the contents of Plaintiff's . . . electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any [s]tate," because the interception violated the FSCA. (Dkt. 1 at 64.) She also claims that Defendant's actions violated the Health Insurance Portability and Accountability Act (HIPAA), (*id.* at 39–44), which makes it unlawful "for a 'covered entity'—which includes health[]care providers—to knowingly disclose individually identifiable hea[l]th information without authorization 'with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.'" *Cooper v. Mount Sinai Health Sys., Inc.*, 742 F. Supp. 3d 369, 379 (S.D.N.Y. 2024) (quoting 42 U.S.C. § 1320d-6). Defendant contends that these allegations are

insufficient because the tortious or criminal purpose must be independent from the interception itself and Plaintiff "cannot restate alleged violations of HIPAA as violations of the [f]ederal Wiretap Act to manufacture a private right of action that does not exist." (Dkt. 17 at 14–16.) Plaintiff responds that the crime-tort exception "requir[es] only 'sufficient facts to support an inference that the offender intercepted the communication for the purpose of a tortious or criminal act that is independent of the intentional act of recording'" and that "'if, at the time of the recording, the offender *plans* to use the recording to harm the other party to the conversation, a civil cause of action exists under the Wiretap Act.'" (Dkt. 20 at 10–11 (quoting *Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010)).) The court agrees with Plaintiff.

Both parties have amassed considerable persuasive—but no binding—authority on this issue. (*See* Dkt. 17 at 13; Dkt. 20 at 8.) *See, e.g.*, *B.K. v. Eisenhower Med. Ctr.*, 721 F. Supp. 3d 1056, 1065 (C.D. Cal. 2024) (determining that the crime-tort exception did not apply to the plaintiff's claims); *Okash v. Essentia Health*, No. 23-482 (JRT/LIB), 2024 WL 1285779, at *4–5 (D. Minn. Mar. 26, 2024) (same); *but see, e.g.*, *Cooper*, 742 F. Supp. 3d at 380 ("A defendant's criminal or tortious purpose of knowingly disclosing individually identifiable health information to another person in violation of HIPAA may satisfy the crime-tort exception." (cleaned up)); *see also Murphy v. Thomas Jefferson Univ. Hosps., Inc.*, No. 22-4674, 2024 WL 4350328, at *5 (E.D. Pa. Sept. 30, 2024) ("[The d]efendant additionally argues that financial motives are not sufficient to prove an intent to tortiously injure [the p]laintiffs. But [the p]laintiffs need not plead financial motive to invoke the crime-tort exception as they have already

sufficiently pleaded [the d]efendant's intention to violate HIPAA. [The p]laintiffs' [Wiretap Act] claim will proceed." (footnote omitted)). While Defendant does cite one Eleventh Circuit decision, (Dkt. 17 at 14–15), that decision is unpublished and supports only the unremarkable proposition that the crime-tort exception applies only to crimes and torts and not to "other injurious act[s]" as a previous iteration of the Wiretap Act did. *Lucas v. Fox News Network, LLC*, No. 00-14519, 2001 WL 100181, at *4 & n.3 (11th Cir. Jan. 16, 2001).

Plaintiff alleges that Defendant intercepted the contents of her communications for the purposes of violating the FSCA and HIPAA. (Dkt. 1 at 39–44, 64–65.) The court finds no basis in the text of the Wiretap Act's crime-tort exception to conclude that these allegations are insufficient. Moreover, given the lack of binding authority and the split in persuasive authority on this issue, the court will not dismiss Plaintiff's allegations while her case is in its infancy. *See Sartori v. Schrodt*, No. 3:18cv204-RV/CJK, 2018 WL 11209992, at *2 (N.D. Fla. May 22, 2018) ("In the absence of binding caselaw, it is enough to say that a 'complicated issue' which generates 'much debate' and a 'split of authority' necessarily states a plausible claim for motion to dismiss purposes."); *Palmyra Park Hosp., Inc. v. Phoebe Putney Mem'l Hosp., Inc.*, No. 1:08-CV-102 (WLS), 2009 WL 10673436, at *6 (M.D. Ga. Mar. 31, 2009) ("[T]he [c]ourt thinks it is a better approach to save the novel issue presented to the [c]ourt for a later day with a more complete record, especially considering the present status of this litigation and the low burden necessary to survive a motion to dismiss.").

Application of the crime-tort exception appears more fit for resolution at summary judgment or trial than at the motion to dismiss stage. *See In re Grp. Health Plan Litig.*, 709 F. Supp. 3d at 720 ("This case is at the pleading stage. While [the p]laintiffs have alleged [the defendant's] motivations, determination of [the defendant's] *actual* purpose for installing and using the Pixel Code requires a factual undertaking. [The p]laintiffs, without the benefit of discovery, have met the pleading requirements to plausibly allege [that] the crime-tort exception applies."); *Cooper*, 742 F. Supp. 3d at 381 ("[The defendant] will be at liberty to attempt to establish in discovery facts supporting, *inter alia*, that, to the extent it took the above actions, it did so without intending to facilitate Facebook's receipt of confidential patient information or to financially benefit. . . . But, taking the [complaint]'s allegations as true, as the [c]ourt must at the motion to dismiss stage, they plausibly support the inference that [the defendant], for commercial ends, intentionally disclosed individually identifiable patient health information[] and thus violated HIPAA . . . ." (footnote omitted)). Indeed, courts in the Northern and Middle Districts of Florida have likewise declined to dismiss Wiretap Act claims in cases asserting virtually identical arguments at the motion to dismiss stage. *See Tallahassee Mem'l Healthcare*, 2024 WL 2318621, at *1; *Cyr*, No. 8:23-cv-588-WFJ-CPT, Dkt. 37. For all of these reasons, the court denies Defendant's motion to dismiss Plaintiff's Wiretap Act claim.

C. Breach of Confidence

A common law breach of confidence claim requires an "unconsented, unprivileged disclosure to a third party of nonpublic information that the defendant

has learned within a confidential relationship." *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 932 (11th Cir. 2020) (en banc) (quotation omitted); *Desue v. 20/20 Eye Care Network, Inc.*, No. 21-CIV-61275-RAR, 2022 WL 796367, at *9 (S.D. Fla. Mar. 15, 2022) (same); *cf. Gracey v. Eaker*, 837 So. 2d 348 (Fla. 2002) (recognizing a cause of action for breach of fiduciary duty in the medical context when a healthcare provider has disclosed confidential information to a third party). Defendant argues that Plaintiff fails to "plead facts sufficient to show that any of her alleged medical information provided in the course of a doctor-patient relationship was actually transmitted to Facebook, Google, or any other third party." (Dkt. 17 at 17.) Defendant also argues that the information "allegedly being sent to Facebook and Google is merely internet metadata automatically generated as a function of a person's browsing activities or the searching of information and not any actual doctor-patient communications." (*Id.* at 19.)

However, Plaintiff alleges that the tracking tools on Defendant's website intercepted her protected health information and transmitted it to Meta and Google. (*Id.* at 35–38.) She specifically alleges that she used Defendant's website "to find gastroenterologists and cardiologists," and in so doing, "she communicated her [protected health information] related to ileostomy, heart pains, fatty liver disease, blacking out when standing up, and meningiomas to find doctors and information concerning these medical conditions and symptoms." (*Id.* at 35.) Her complaint includes exhaustive detail as to how exactly the tracking tools Defendant installed on its website intercepted her health information. (*Id.* at 18–34.) Moreover, Plaintiff

includes allegations supporting the interception of her medical information. Specifically, she alleges that after communicating this information to Defendant she received advertisements on Facebook for products and services related to the medical conditions referenced in her communications with Defendant's website. (*Id.* at 36–38.) Therefore, the information Plaintiff alleges she shared with Defendant through its website was not merely "metadata" but was rather information directly related to her status as Defendant's patient and to her health. *See Norman-Bloodsaw v. Lawrence Berkeley Lab'y*, 135 F.3d 1260, 1269 (9th Cir. 1998) ("One can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health . . . ."); *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 799 (N.D. Cal. 2022) ("[U]nlike communications made while inquiring about items of clothing on a retail website, health-related communications with a medical provider are almost uniquely personal." (citation omitted)).

Accordingly, Plaintiff's allegations are sufficient to state a claim for breach of confidence, and Defendant's motion as to this claim is denied. *See Tallahassee Mem'l Healthcare*, 2024 WL 2318621, at *1; *Cyr*, No. 8:23-cv-588-WFJ-CPT, Dkt. 37.

D. Invasion of Privacy—Intrusion Upon Seclusion

Florida recognizes a common law claim of intrusion upon seclusion—one form of the tort of invasion of privacy—which it defines as an intrusion "physically or electronically . . . into one's private quarters." *Allstate Ins. Co. v. Ginsberg*, 863 So. 2d 156, 162 (Fla. 2003) (quotation omitted). This tort requires intrusion "into a 'place' in

which there is a reasonable expectation of privacy," *id.*, which intrusion must be "highly offensive to a reasonable person," *Jackman v. Cebrink-Swartz*, 334 So. 3d 653, 656 (Fla. Dist. Ct. App. 2021) (quoting Restatement (Second) of Torts § 652B (Am. L. Inst. 1977)); *see Rebalko v. City of Coral Springs*, 552 F. Supp. 3d 1285, 1332 (S.D. Fla. 2020) ("An intrusion claim has three elements. First, there must be a private quarter. Second, there must be some physical or electronic intrusion into that private quarter. Third, the intrusion must be highly offensive to a reasonable person." (quotation omitted)).

Defendant argues that Plaintiff has failed to state a claim for intrusion upon seclusion because she does not allege an intrusion into her private quarters. (Dkt. 17 at 20.) The court agrees. "Florida law explicitly requires an intrusion into a private place and not merely into a private activity." *Pet Supermarket, Inc. v. Eldridge*, 360 So. 3d 1201, 1207 (Fla. Dist. Ct. App. 2023) (quoting *Spilfogel v. Fox Broad. Co.*, 433 F. App'x 724, 727 (11th Cir. 2011)). This standard is met where a plaintiff's home is intruded into. *Cf. Jackman*, 334 So. 3d at 655–57 (finding the plaintiffs had demonstrated a substantial likelihood of success on the merits of their intrusion upon seclusion claim where the defendants had installed a camera "positioned to see over the [plaintiffs]' [six-foot-high] privacy fence, allowing the [defendants] to see into a portion of the [plaintiffs]' backyard and the edge of their lanai"). An intrusion that occurs in a public setting, on the other hand, does not satisfy this standard. *See Rebalko*, 552 F. Supp. 3d at 1332–33 (determining that "a police officer's stop at the intersection of a public street—in full view of dozens of motorists and other passersby" was not an

intrusion into a plaintiff's private quarters). Florida courts have not identified all of the settings qualifying as a private place. *See id.* at 1332 ("Although a person's home plainly constitutes a private quarter, Florida's courts have said precious little about what else might qualify." (cleaned up)).

Plaintiff argues that Defendant intruded into her private quarters because its tracking tools intruded into her web browser "conversations with [her] healthcare providers." (Dkt. 20 at 15–16.) She points to no authority, however, demonstrating that such internet activity constitutes an intrusion into one's private quarters under Florida law. (*See id.* at 15–17.) Defendant, however, has identified caselaw that indicates the contrary. (*See* Dkt. 17 at 20 (citing *Bradley v. City of St. Cloud*, No. 6:12-cv-1348-Orl-37TBS, 2013 WL 3270403, at *4–5 (M.D. Fla. June 26, 2013) (dismissing an intrusion upon seclusion claim based on "allegations that [a defendant] investigated [the plaintiff] and viewed her medical records[] at [a] hospital . . . without her authorization" because the plaintiff had "not allege[d] that [the d]efendants intruded into her home or another private place"), and *Watts v. City of Hollywood*, 146 F. Supp. 3d 1254, 1267–68 (S.D. Fla. 2015) ("The [defendant]'s accessing of [the plaintiff]'s driver's license information in the [Driver and Vehicle Information Database (DAVID)] system is likewise not an intrusion into a 'place.' [The plaintiff]'s attempt to liken the archiving of her information in DAVID to the keeping of personal effects in a home safe or desk drawer is both unsupported and unpersuasive. Similarly, [the plaintiff]'s argument 'her privacy was invaded electronically, and included the private

information about her physical domains of home and vehicle,' . . . is not supported by a single citation to legal authority . . . ." (citations omitted))).)

Plaintiff's attempt to distinguish *Watts* on the basis of the substance of the information at issue is unavailing. (*See* Dkt. 20 at 16 ("*Watts* addressed driver license records—not private, sensitive, and confidential medical information.").) The *Watts* court found no "place" to be implicated not because of the contents of the information at issue, but because it found the plaintiff had no reasonable expectation of privacy in the *location* of that information—a database owned by the state. *See Watts*, 146 F. Supp. 3d at 1267. The *Bradley* court articulated this same understanding, finding an unauthorized viewing of medical records did not constitute an intrusion upon the plaintiff's seclusion "[b]ecause [the p]laintiff d[id] not allege that [the d]efendants intruded into her home or another private place." 2013 WL 3270403, at *4–5.

Plaintiff's allegations demonstrate that her claim is based on an intrusion into private activities, rather than a private place, and therefore, her claim is not cognizable under Florida law. (*See* Dkt. 1 at 68–69 (alleging Defendant violated Plaintiff's privacy because "it installed the [t]racking [t]ools onto its [w]ebsite . . . to disseminate patient[s'] *communications with the* [*w*]*ebsite*").) *See Hammer v. Sorensen*, 824 F. App'x 689, 695 (11th Cir. 2020) ("[T]he Supreme Court of Florida has construed the tort of intrusion upon seclusion even more narrowly than the Restatement . . . [and i]t has required a plaintiff to show an intrusion into a private place and not merely a private activity." (citation omitted)).

Aside from *Jackman*, which is distinguishable, Plaintiff cites no authority to demonstrate that Florida would recognize an intrusion upon seclusion claim based on the facts alleged in her complaint. (*See* Dkt. 20 at 15–17.) *Cf. Spilfogel*, 433 F. App'x at 726–27 (affirming the district court's dismissal of an intrusion upon seclusion claim where the "[p]laintiff fail[ed] to produce any meaningful support for her argument" because she "cite[d] to no Florida cases whatsoever in support of her intrusion upon seclusion claim"); *Rebalko*, 552 F. Supp. 3d at 1333 (dismissing intrusion upon seclusion claims with prejudice where the intrusion did not appear to implicate the plaintiffs' private quarters and they "pointed the court to *no* authority that would suggest otherwise").

Accordingly, Defendant's motion is granted as to this claim. While leave to amend may be futile, the court will nevertheless grant Plaintiff leave to amend her complaint to replead an invasion of privacy claim in light of the strong federal policy favoring amendment. *See* Fed. R. Civ. P. 15(a)(2) ("The court should freely give leave [to amend a pleading before trial] when justice so requires.").

E. Unjust Enrichment

Under Florida law, the "essential" elements of a claim for unjust enrichment are "(1) a benefit conferred upon a defendant by the plaintiff, (2) the defendant's appreciation of the benefit, and (3) the defendant's acceptance and retention of the benefit under circumstances that make it inequitable for him to retain it without paying the value thereof." *Vega v. T-Mobile USA, Inc.*, 564 F.3d 1256, 1275 (11th Cir. 2009) (quoting *Rollins, Inc. v. Butland*, 951 So. 2d 860, 876 (Fla. Dist. Ct. App. 2006)).

Defendant contends that Plaintiff has failed to plead that a benefit was conferred upon Defendant. (Dkt. 17 at 21–22.) Plaintiff, however, alleges that she "conferred a benefit upon Defendant in the form of [p]rivate [i]nformation that Defendant collected from Plaintiff . . . without authorization [or] proper compensation," and that Defendant "consciously collected and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation." (Dkt. 1 at 70.) Moreover, she specifically alleges that her private information "has economic value." (*Id.* at 48–50.) The court agrees that private information, at least in the context of sensitive medical information, has value. *See In re Marriot Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the [c]ourt ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. . . . Consumers too recognize the value of their personal information and offer it in exchange for goods and services."). Moreover, in the context of an unjust enrichment claim, "whether a defendant benefitted at the plaintiff's expense . . . 'is a factual question not appropriately resolved on a motion to dismiss.'" *Daniel v. Navient Sols., LLC*, 328 F. Supp. 3d 1319, 1326 (M.D. Fla. 2018) (quoting *Shands Teaching Hosp. & Clinics, Inc. v. Beech St. Corp.*, 899 So. 2d 1222, 1228 (Fla. Dist. Ct. App. 2005)).

Defendant states that Plaintiff's unjust enrichment claim must be dismissed "because courts routinely recognize that allegations of collection and dissemination of website usage information are insufficient to establish an uncompensated benefit as

needed to support a claim for unjust enrichment." (Dkt. 17 at 22–23.) The court finds this argument unpersuasive both because the information at issue here is not merely "website usage information" and because Defendant cites no controlling law to illustrate that Florida courts would not recognize Plaintiff's allegations as constituting a benefit conferred. (*See id.*) The court finds Plaintiff's allegations sufficient to state an unjust enrichment claim under Florida law. Accordingly, the court denies Defendant's motion to dismiss this claim. *See also Tallahassee Mem'l Healthcare*, 2024 WL 2318621, at *1; *Cyr*, No. 8:23-cv-588-WFJ-CPT, Dkt. 37.

F. Breach of Implied Contract

To the extent that Plaintiff asserts a claim for breach of contract implied in law, the claim survives for the reasons explained above in connection with Plaintiff's unjust enrichment claim. *See Com. P'ship 8098 Ltd. P'ship v. Equity Contracting Co.*, 695 So. 2d 383, 386 (Fla. Dist. Ct. App. 1997) (noting that "unjust enrichment" is one of several terms used to describe a contract implied in law). Following the parties' lead, (*see* Dkt. 17 at 23–25; Dkt. 20 at 19–21), the court treats Plaintiff's claim for breach of implied contract as a claim for breach of contract implied in fact.

"A contract implied in fact is one form of an enforceable contract; it is based on a tacit promise, one that is inferred in whole or in part from the parties' conduct, not solely from their words." *SBP Homes, LLC v. 84 Lumber Co.*, 384 So. 3d 241, 245 (Fla. Dist. Ct. App. 2024) (quoting *Com. P'ship 8098*, 695 So. 2d at 385). Defendant argues that Plaintiff's complaint contains "no allegations that plausibly show that [Defendant] agreed not to use website analytics tools on its publicly accessible website." (Dkt. 17

at 24.) Defendant also argues that Plaintiff has failed to allege damages. (*Id.* at 24–25.) However, arguments as to whether there was a meeting of the minds between the parties, or regarding damages, are generally questions of fact best resolved after discovery. *See Vanguard Plastic Surgery, PLLC v. UnitedHealthcare Ins. Co.*, 658 F. Supp. 3d 1250, 1261–62 (S.D. Fla. 2023) (determining that, under Florida law, "whether there has been a 'meeting of the minds' is a question of fact," and that "whether an implied-in-fact contract has been formed can be a fact-intensive inquiry better resolved after discovery"); *see also In re Grp. Health Plan Litig.*, 709 F. Supp. 3d at 715 ("Arguments about whether [the p]laintiffs and [the defendant] had a meeting of the minds or debates over the value of [the p]laintiffs' loss[es] are fact disputes better left for summary judgment or trial."). Moreover, Florida law permits a breach of contract claim to proceed even absent proof of quantifiable damages, because the plaintiff in such a case would still be entitled to nominal damages if she established a breach. *See AMC/Jeep of Vero Beach, Inc. v. Funston*, 403 So. 2d 602, 605 (Fla. Dist. Ct. App. 1981) ("While there is a legal remedy for every legal wrong and, thus, a cause of action exists for every breach of contract, an aggrieved party who has suffered no damage is only entitled to a judgment for nominal damages.").

Defendant's motion to dismiss this claim is thus denied. *See Tallahassee Mem'l Healthcare*, 2024 WL 2318621, at *1; *Cyr*, No. 8:23-cv-588-WFJ-CPT, Dkt. 37.

CONCLUSION

Accordingly:

1. Defendant Orlando Health, Inc.'s Motion to Dismiss Plaintiff's Complaint (Dkt. 17) is **GRANTED in part and DENIED in part**. Count IV is **DISMISSED without prejudice**. Defendant's motion is otherwise **DENIED**.
2. Plaintiff may file an amended complaint on or before March 21, 2025.
3. If Plaintiff amends, Defendant's response is due on or before April 4, 2025.

ORDERED in Orlando, Florida, on March 6, 2025.

JULIE S. SNEED
UNITED STATES DISTRICT JUDGE

Copies furnished to:
Counsel of Record