UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

JANE DOE, et al., Plaintiffs, v. WELLSTAR HEALTH SYSTEM, INC., Defendant.	CIVIL ACTION NO. 1:24-CV-01748-JPB

ORDER

This matter comes before the Court on Wellstar Health System, Inc.'s ("Defendant") Motion to Dismiss [Doc. 23]. The Court finds as follows:

BACKGROUND

The facts of this case, taken from the Amended Complaint, are as follows. Jane Doe, Jane Doe #2, Jane Doe #3 and John Doe (collectively, "Plaintiffs") bring this putative class action on behalf of themselves and "all others similarly situated" alleging several claims under state and federal law. [Doc. 20, pp. 1–2]. Plaintiffs are individuals who have used Defendant's website and patient portal since as early as 2007 to seek medical treatment. Id. at 92–105. Defendant is "one of the largest health systems in the state of Georgia," serving millions of patients annually and is a covered entity under the Health Insurance Portability and

Accountability Act of 1996 ("HIPAA"). Id. at 14. Defendant maintains a website at https://www.wellstar.org/ and a patient portal known as Wellstar MyChart at mychart.wellstar.org (collectively, the "Web Properties"). Id. at 2.

According to Plaintiffs, Defendant "encouraged and/or required patients to use" the Web Properties "in conjunction with seeking and receiving healthcare services." Id. at 16. While using the Web Properties, Plaintiffs claim they were required to disclose personally identifiable information ("PII") and protected health information ("PHI"). Id. Plaintiffs allege that, without their knowledge or permission, Defendant utilized Google and Meta data collection tools on its Web Properties "to share patients' confidential information including" PII and PHI "with Meta, Google, and other unauthorized third parties." Id. at 2, 16. Plaintiffs assert that Defendant began to use Google tools as early as 2008 and Meta tools as early as June 2016 through at least June 2022, disclosing private information to Meta and Google throughout this period. Id. at 16, 42. Indeed, Plaintiffs claim that Defendant

> intentionally configured the Google and Meta Collection Tools installed on the Web Properties to capture both the "characteristics" of individual patients' communications with the . . . Web Properties (e.g., their IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers) and the "content" of these communications (i.e., the buttons, links, pages, and tabs they click and view, as well as search terms entered into free text boxes and descriptive URLs showing the information being exchanged).

Id. at 19. Moreover, Plaintiffs contend that Defendant employed tools such as Meta Pixel to analyze patients' activity on the Web Properties so that Defendant could better target patients with ads based on their online behavior. Id. at 23–24. For instance, Plaintiffs claim that, if a patient searched for a specific medical condition in the patient portal, Meta Pixel could transmit that information to Defendant and link the information to the patient's Facebook profile, allowing Defendant to later target that patient with specific ads on Facebook related to his or her previous search. Id. at 52–53, 88.

Plaintiffs contend that, by choosing to install the Meta Pixel tool on its Web Properties, Defendant ensured that patients' activity on the Web Properties was "contemporaneously redirected to Meta." Id. at 25. Plaintiffs claim that Defendant disclosed information to Meta such as: when a patient would click to register for the patient portal; information that a patient typed into the registration form (name, email address and zip code); when a patient logged into their patient portal; when a patient scheduled an appointment; information that a patient typed into an appointment form; when a patient clicked a button to call their provider from Defendant's website; descriptive URLs detailing where patients navigated within the Web Properties; the nature of patients' clicks on categories within the Web Properties; the communications a patient exchanged through the Web Properties;

and similar communications between patients and health insurance companies, pharmacies and prescription drug companies. Id. at 28–29. Likewise, Plaintiffs allege that Defendant employed Google Analytics to collect data concerning patients' actions on the Web Properties and transmit the information to Google to optimize Defendant's advertising. Id. at 37.

Plaintiffs further assert that "Defendant's privacy policies represent to Plaintiffs and Class Members that Defendant will keep Private Information . . . confidential, and it will only disclose Private Information under certain circumstances." Id. at 62. Nevertheless, Plaintiffs claim that Defendant used Google and Meta tools on its Web Properties to transmit PII and PHI to third parties in violation of its own privacy policies and without patients' knowledge or consent. Id. at 64–66. Plaintiffs allege that, "[i]n exchange for disclosing the PII of its patients, Defendant is compensated by Google and Facebook in the form of enhanced advertising services and more cost-efficient marketing." Id. at 88.

From these factual allegations, Plaintiffs bring the following claims against Defendant: invasion of privacy—intrusion upon seclusion (Count I); breach of fiduciary duty (Count II); negligence (Count III); negligence per se (Count IV); breach of implied contract (Count V); breach of express contract (Count VI); unjust enrichment (Count VII); and violation of the Electronic Communications

Privacy Act, 18 U.S.C. § 2511, *et seq.* ("ECPA") (Count VIII). Id. at 113–43. Plaintiffs seek class certification, equitable relief, monetary damages, attorneys' fees and the costs of litigation. Id. at 143–144. In response to Plaintiffs' Amended Complaint, Defendant filed a Motion to Dismiss, requesting that the Court dismiss each count pursuant to Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim upon which relief can be granted. [Doc. 23]. Plaintiffs oppose Defendant's Motion. [Doc. 27].

LEGAL STANDARD

"At the motion to dismiss stage, all well-pleaded facts are accepted as true, and the reasonable inferences therefrom are construed in the light most favorable to the plaintiff." Bryant v. Avado Brands, Inc., 187 F.3d 1271, 1273 n.1 (11th Cir. 1999). In determining whether this action should be dismissed for failure to state a claim, Federal Rule of Civil Procedure 8(a)(2) provides that a pleading must contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Although detailed factual allegations are not necessarily required, the pleading must contain more than "'labels and conclusions' or 'a formulaic recitation of the elements of a cause of action.'" Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007)). Importantly, "a complaint must contain sufficient factual matter, accepted

as true, to 'state a claim to relief that is plausible on its face.'" Id. (quoting Twombly, 550 U.S. at 570).

ANALYSIS

Defendant asks the Court to dismiss each of Plaintiffs' claims, arguing that Plaintiffs have wholly failed to state a claim under both federal and state law. [Doc. 23, p. 1].

I. Plaintiffs' Claim for Invasion of Privacy (Count I)

In Count I, Plaintiffs contend that Defendant's surreptitious tracking and transmission of their data on the Web Properties was an invasion of privacy under Georgia law. [Doc. 20, pp. 113–15]. Defendant argues this claim fails as a matter of law because Plaintiffs do not allege that Defendant, rather than a third party, intruded upon Plaintiffs' privacy. [Doc. 23-1, p. 16]. Defendant also asserts that Plaintiffs do not adequately allege that the disclosure at issue was highly offensive or publicized "beyond a discrete number of third parties in a manner that would be actionable." Id. at 17. Plaintiffs respond that they adequately allege Defendant invaded their privacy by installing data tracking tools on its Web Properties to which Plaintiffs did not consent. [Doc. 27, pp. 18–20].

Intrusion upon seclusion is one of four categories of invasion of privacy claims in Georgia, and it "involves a prying or intrusion, which would be offensive

or objectionable to a reasonable person, into a person's private concerns." Welch v. Citibank, N.A., No. 15-CV-3618, 2016 WL 11567853, at *6 (N.D. Ga. Sept. 8, 2016) (quoting Yarbray v. S. Bell Tel. & Tel. Co., 409 S.E.2d 835, 837 (Ga. 1991)). "An essential element of this tort is a physical intrusion analogous to a trespass." Welch, 2016 WL 11567853, at *6. The element of trespass may be met by alleging that the defendant "conducted surveillance on the plaintiff or otherwise monitored her activities." Benedict v. State Farm Bank, FSB, 709 S.E.2d 314, 318 (Ga. Ct. App. 2011) (quoting Anderson v. Mergenhagen, 642 S.E.2d 105, 109 (Ga. Ct. App. 2007)). Moreover, "[t]he unreasonable intrusion aspect of the invasion of privacy involves a prying or intrusion, which would be offensive or objectionable to a reasonable person, into a person's private concerns." Miller v. NextGen Healthcare, Inc., 742 F. Supp. 3d 1304, 1315 (N.D. Ga. 2024) (citation modified).

Where, as here, Plaintiffs voluntarily provided their information to Defendant, there is no intrusion upon seclusion. See T.D. v. Piedmont Healthcare, Inc. (*T.D. I*), No. 23-CV-5416, 2024 WL 3972984, at *2 (N.D. Ga. Aug. 28, 2024) (finding that "[t]here is no intrusion upon privacy when a patient voluntarily provides personally identifiable information and protected health information to his or her healthcare provider" and collecting cases). Here, Plaintiffs assert that Defendant committed the tort of invasion of privacy by allowing data collection

tools to track patients' activity on Defendant's Web Properties. [Doc. 20, p. 114]. However, it is undisputed that Plaintiffs voluntarily shared their information with Defendant, and third parties' receipt of the information does not constitute an invasion *by Defendant*. See Purvis v. Aveanna Healthcare, LLC, 563 F. Supp. 3d 1360, 1377–78 (N.D. Ga. 2021) (finding that the plaintiffs failed to state a claim for invasion of privacy based on a third-party data breach because they did not allege that the defendant—as opposed to the third party—improperly surveilled or trespassed upon their property); Allen v. Novant Health, Inc., No. 22-CV-697, 2023 WL 5486240, at *2 (M.D.N.C. Aug. 24, 2023) ("Because the plaintiffs acknowledge in the complaint that they voluntarily provided their information directly to [the defendant], . . . they have not alleged an intrusion or unauthorized prying."). Accordingly, to the extent Defendant seeks dismissal of Plaintiffs' claim for invasion of privacy, Defendant's motion is **GRANTED** and the claim is dismissed with prejudice.

II. Plaintiffs' Claims for Breach of Fiduciary Duty, Breach of Contract and Negligence (Counts II–VI)

In Counts II through VI, Plaintiffs allege claims for breach of fiduciary duty, negligence, negligence per se, breach of implied contract and breach of express contract. [Doc. 20, pp. 116–32]. Defendants offer several arguments for dismissal of these claims, among which is the assertion that Plaintiffs fail to adequately

allege damages, a required element of each of these claims. See [Doc. 23-1, pp. 19, 22, 29]. In response, Plaintiffs argue that other courts have recognized theft of sensitive personal data, loss of value of private information and loss of the benefit of the bargain as legally actionable damages. See [Doc. 27, pp. 31–34] (citing several cases from other jurisdictions where courts found similar damages theories viable). Plaintiffs also contend that their allegations of emotional distress, embarrassment, humiliation and loss of enjoyment constitute valid damages under Georgia law. Id. at 35.

Courts in Georgia have found it

> well-established . . . that before an action for a tort will lie, the plaintiff must show he sustained injury or damage as a result of the negligent act or omission to act in some duty owed to him. Although nominal damages can be awarded where there has been an injury but the injury is small, . . . where there is no evidence of injury accompanying the tort, an essential element of the tort is lacking, thereby entitling the defendant to judgment in his favor.

In re Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1315 (N.D. Ga. 2019) (citation modified).

Here, the Court is not persuaded that Plaintiffs adequately allege damages in a non-speculative, non-conclusory fashion. Plaintiffs' damages allegations in their Amended Complaint largely mirror those pled by the plaintiffs in T.D. Compare 2024 WL 3972984, at *3 (reciting the damages allegations in the plaintiffs'

complaint) with [Doc. 20, pp. 95, 98, 101, 104] (listing similar damages allegations as to each individual Plaintiff in the instant action). In T.D., the district court described the plaintiffs' damages allegations as repetitive and conclusory and found that the plaintiffs failed to allege actual (as opposed to hypothetical) harm or facts from which the court could trace the purported harm to the defendant's alleged wrongdoing. 2024 WL 3972984, at *3. The Court finds that Plaintiffs' Amended Complaint here suffers from the same deficiencies.

Further, while Plaintiffs attempt to shore up their damages allegations by directing the Court's attention to other jurisdictions where courts have allowed similar damages theories to proceed, Plaintiffs fail to confront the persuasive authorities in this district foreclosing such theories. See, e.g., Everhart v. Colonial Pipeline Co., No. 21-CV-3559, 2022 WL 3699967, at *2–5 (N.D. Ga. July 22, 2022) (rejecting the plaintiffs' damages allegations based on diminished value of PII, mitigation expenses due to unauthorized use of PII, continued risk to PII and opportunity costs associated with mitigation expenses); Provost v. Aptos, Inc., No. 17-CV-02120, 2018 WL 1465766, at *4 (N.D. Ga. Mar. 12, 2018) ("The Court is not persuaded by the hypothetical diminution of value propounded by [the p]laintiff. [The p]laintiff has failed to allege with particularity any facts explaining

how her personal identity information is less valuable than it was before the [data b]reach.").[1]

Additionally, although Plaintiffs argue that the damages of "emotional distress, embarrassment, humiliation and loss of enjoyment of life . . . are well supported in Georgia," Plaintiffs' allegations of emotional damage fail to extend beyond a handful of conclusory statements. [Doc. 27, p. 35]; see [Doc. 20, pp. 119, 124] ("Plaintiffs and the Class have suffered damages that include . . . embarrassment, emotional distress, humiliation and loss of enjoyment of life."). Moreover, Plaintiffs do not explain how the dissemination of their PII and PHI to third parties and Defendant's targeted ads are linked to such damages. Heinen v. Royal Caribbean Cruises Ltd., 806 F. App'x 847, 850 (11th Cir. 2020) ("Because the appellants fail to connect their general allegations of 'physical and emotional

[1] Plaintiffs argue that "[u]nlike what this Court found lacking in the damages pled in [Provost v. Aptos], Plaintiffs *expressly plead* that they *relied on* [Defendant's] representations in its Privacy Notice that [Defendant] *would not share* their Private Information with unauthorized third parties." [Doc. 27, p. 34]. However, the Court finds Plaintiffs' attempt to distinguish Provost ineffective. In Provost, the plaintiff alleged that, "had [the d]efendants told her that [they] lacked adequate computer systems and data security practices to safeguard customers' Personal Information from theft," she would not have used her debit card to make purchases on the defendant's website—an act which the plaintiff identified as the cause of her injury. 2018 WL 1465766, at *1. Nevertheless, the court in Provost found that the plaintiff's allegations of lost benefit of the bargain, diminution in value of PII and increased risk to PII were insufficient to establish Article III standing. Id. at *3–6.

damage' with the specific facts pleaded in bulk, we must ignore that threadbare assertion of harm.").

Accordingly, the Court finds that Plaintiffs have failed to state plausible claims for breach of fiduciary duty, breach of express and implied contract, negligence and negligence per se—all of which include the required element of damages. Thus, to the extent Defendant seeks dismissal of these claims, Defendant's Motion to Dismiss is **GRANTED** and the Court finds these claims should be dismissed without prejudice.

III. Plaintiffs' Unjust Enrichment Claim (Count VII)

In the Amended Complaint, Plaintiffs further assert a claim for unjust enrichment. Plaintiffs argue that they "conferred a benefit upon Defendant" by providing Defendant with their PII and that Defendant exceeded the scope of Plaintiffs' permission by sharing the information with third parties. [Doc. 20, p. 133]. In return for sharing their private information, Plaintiffs allege that Defendant was "compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on Facebook." Id. In response, Defendant contends that Plaintiffs fail to state a claim for unjust enrichment because their allegations are conclusory, because Plaintiffs did not allege why the benefit purportedly retained by Defendant required compensation and because

Plaintiffs received a benefit in return—namely, access to the Web Properties and medical treatment. [Doc. 23-1, pp. 30–31].

"A claim of unjust enrichment will lie if there is no legal contract and the party sought to be charged has been conferred a benefit by the party contending an unjust enrichment which the benefitted party equitably ought to return or compensate for." Campbell v. Ailion, 790 S.E.2d 68, 73 (Ga. Ct. App. 2016) (quoting Jones v. White, 717 S.E.2d 322, 328 (Ga. Ct. App. 2011)). Unjust enrichment is "premised upon the principle that a party cannot induce, accept, or encourage another to furnish or render something of value to such party and avoid payment for the value received." Campbell, 790 S.E.2d at 73 (quoting Jones, 717 S.E.2d at 328). Thus, to prevail on a claim for unjust enrichment, a plaintiff must ultimately show "(1) that it conferred a benefit on the defendant and (2) that equity requires the defendant to compensate for that benefit." Brooks v. Branch Banking & Tr. Co., 107 F. Supp. 3d 1290, 1298 (N.D. Ga. 2024) (quoting Shutz Container Sys., Inc. v. Mauser Corp., No. 09-CV-3609, 2012 WL 1073153, at *35 (N.D. Ga. Mar. 28, 2012)).

Here, Plaintiffs allege that Defendant went beyond the scope of patients' permission by using data tracking tools to transmit their PII and PHI to third parties such as Meta and Google so that Defendant could improve its advertising.

Examining the allegations in the Amended Complaint in the light most favorable to Plaintiffs, the Court finds that they adequately plead a claim for unjust enrichment. See W.W. v. Orlando Health, Inc., No. 24-CV-1068, 2025 WL 722892, at *10 (M.D. Fla. Mar. 6, 2025) (finding that the plaintiffs sufficiently alleged a claim for unjust enrichment under Florida law where they claimed the defendant wrongfully harvested patient data from its medical portal and exchanged that information in return for its own gain). Moreover, to the extent Defendant argues that Plaintiffs' claim fails because they received a benefit in the form of access to the Web Properties and medical treatment, the Court finds this argument unpersuasive. Plaintiffs assert that they provided Defendant with their PII and PHI in reliance on Defendant's privacy policy, wherein Defendant agreed not to share patient data for such purposes absent consent. See, e.g., [Doc. 20, p. 94] ("In reliance on Defendant's Notice of Privacy Practices, [Jane Doe] provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies in addition to state and federal law."). Thus, Plaintiffs sufficiently allege that they provided Defendant with benefits they did not intend to confer and for which they were not compensated.

Accordingly, to the extent Defendant seeks dismissal of Plaintiffs' unjust enrichment claim, the Motion to Dismiss is **DENIED**.

IV. Plaintiffs' ECPA Claim (Count VIII)

In Count VIII, Plaintiffs allege that Defendant violated the ECPA, also known as the Wiretap Act, by intercepting Plaintiffs' communications on the Web Properties and transmitting those communications to third parties. [Doc. 20, pp. 134–43]. The Wiretap Act "prohibits the unauthorized interception of electronic communication and intentional disclosure or use of the contents of an intercepted communication." In re Group Health Plan Litig., 709 F. Supp. 3d 707, 717 (D. Minn. 2023) (citing 18 U.S.C. § 2511(1)(a), (c), (d)). To state a successful ECPA claim, a plaintiff must sufficiently allege that the defendant (1) intentionally (2) intercepted (3) the contents of (4) an electronic communication (5) using a device. Hamilton Grp. Funding, Inc. v. Basel, 311 F. Supp. 3d 1307, 1314 (S.D. Fla. 2018).

The Wiretap Act only requires the consent of one party to a communication; thus, under the "party exception," if the person intercepting a communication "is a party to the communication or where one of the parties to the communication has given prior consent to such interception," no violation occurs. 18 U.S.C. § 2511(2)(d). However, the party exception is itself limited by the "crime-tort exception," which provides that a party can 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 State." Id.

Defendant argues that Plaintiffs fail to state a viable claim under the ECPA because they do not properly plead the contents of the communications subject to unlawful transmission, because Plaintiffs cannot show that Defendant unlawfully intercepted communications to which it was a party and finally because the crime-tort exception does not apply. [Doc. 23-1, pp. 8–15]. Plaintiffs respond that they sufficiently describe the contents of the communications at issue and that the crime-tort exception applies because Defendant "intercepted [Plaintiffs'] electronic communications for the purpose of violating HIPAA." [Doc. 27, pp. 8–17].

A. Plaintiffs adequately plead the contents of the communications.

First, Defendant argues that Plaintiffs allege only "non-substantive interactions" with Defendant's Web Properties and otherwise fail to specify the contents of communications comprising their ECPA claim. [Doc. 23-1, p. 18]. However, in their Amended Complaint, Plaintiffs assert that Defendant used Meta and Facebook tools to convey sensitive patient information to third parties, including information patients typed into registration and appointment forms, descriptive URLs detailing where patients navigated within the Web Properties and the descriptive nature of Plaintiffs' searches within the Web Properties. [Doc. 20,

pp. 28–29]. For instance, Plaintiffs claim that the Google and Meta tools conveyed their search terms—including searches for medical conditions and treatments—to third parties without Plaintiffs' knowledge or consent. Id. at 52–53. The Amended Complaint also describes specific allegations as to tasks that Jane Doe, Jane Doe #2 and Jane Doe #3 performed on Defendant's Web Properties, including interacting with providers concerning symptoms and medical conditions, obtaining referrals and viewing test results and doctors' notes. Id. at 92–102.

Section 2510(8) defines "content" to include "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). At the motion to dismiss stage and construing all reasonable inferences in the light most favorable to Plaintiffs, the Court finds that Plaintiffs adequately plead the nature of the contents of their communications because they allege facts supporting the transmission of descriptive, specific information to third parties. See W.W., 2025 WL 722892, at *5–6 (finding the plaintiff stated a claim under the Wiretap Act and Florida's state-law equivalent where the plaintiff alleged that the defendant used Meta and Google tools to disclose—among other information—users' searches concerning sensitive health conditions and products).

B. The party exception applies unless Defendant acted with a criminal or tortious purpose.

Second, Defendant argues that Plaintiffs' ECPA claim fails because a party cannot intercept its own communications. [Doc. 23-1, pp. 9–10]. To the extent Defendant asserts that it was a party to the communications at issue in Plaintiffs' ECPA claim, the Court agrees. Indeed, in their Amended Complaint, Plaintiffs allege that they exchanged communications with Defendant on its Web Properties. See, e.g., [Doc. 20, p. 135] ("Wellstar intentionally intercepted electronic communications that Plaintiffs and Class Members exchanged *with Wellstar* through the Google and Meta Collection Tools installed on Wellstar's Web Properties." (emphasis added)). Thus, because Defendant was a party to the communications, there can be no ECPA violation unless Defendant intercepted the communications for the purpose of committing a crime or tort. 18 U.S.C. § 2511(2)(d).

C. Plaintiffs adequately plead a basis for applying the crime-tort exception.

Defendant argues that Plaintiffs fail to allege a basis for the crime-tort exception because they do not sufficiently plead: (1) the occurrence of a separate criminal or tortious act beyond the interception itself or (2) that Defendant intercepted the communications for a criminal or tortious purpose. [Doc. 23-1, p.

13–14]. As to the first argument, the Court is unpersuaded. Plaintiffs claim that Defendant not only intercepted their communications on the Web Properties by using data tracking tools, but also transmitted the information to third parties such as Meta and Google. [Doc. 20, p. 136]. The Court finds these allegations are sufficient to indicate a separate tortious or criminal act apart from the interception. Regardless of whether the transmission was simultaneous with the interception, the Court finds that, at this stage, Plaintiffs sufficiently plead the existence of a separate act for purposes of applying the crime-tort exception. See R.S. v. Prime Healthcare Servs., Inc., No. 24-CV-00330, 2025 WL 103488, at *5–6 (C.D. Cal. Jan. 13, 2025) (finding it irrelevant that the defendant simultaneously intercepted and disclosed information because the temporal aspect to the crime-tort exception focuses on when the defendant formed the intent to use information in a criminal or tortious way). Here, Plaintiffs claim that Defendant affirmatively chose to implement tools such as Meta Pixel and Google Analytics on its Web Properties, suggesting an "intent to disclose private information [which] predate[d] and [was] distinct from the interception itself." Id., at *5.

As to its second argument, Defendant contends that the crime-tort exception does not apply because Plaintiffs fail to sufficiently allege that Defendant intercepted the communications for a criminal or tortious purpose. [Doc. 23-1, p.

13]. Plaintiffs respond that Defendant acted with the purpose of violating HIPAA; thus, the crime-tort exception applies. [Doc. 27, p. 13].

The crime-tort exception focuses on whether "the *purpose* for the interception—its intended use—was criminal or tortious." In re Meta Pixel Healthcare Litig., 647 F. Supp. 3d 778, 796–97 (N.D. Cal. 2022) (quoting Sussman v. Am. Broad Companies, Inc., 186 F.3d 1200, 1202 (9th Cir. 1999)). "The existence of a lawful purpose does not sanitize an interception that was made for an illegitimate purpose." In re Meta Pixel, 647 F. Supp. 3d at 797. HIPAA makes it unlawful for any covered entity—including healthcare providers—to knowingly "disclose[] individually identifiable health information to another person." 42 U.S.C. § 1320d-6(a)(3). The statute provides additional penalties when a covered entity discloses the information with the intent to use it "for commercial advantage [or] personal gain." Id. at § 1320d-6(b)(3). However, some courts have found that—where a defendant's primary intent is to make money rather than injure the plaintiffs tortiously—the crime-tort exception does not apply. In re Meta Pixel, 647 F. Supp. 3d at 797.

Here, Plaintiffs allege that Defendant captured and transmitted their PII and PHI to third parties without their consent and in violation of Defendant's own privacy policies and HIPAA. [Doc. 20, pp. 64–65]. At the motion to dismiss

stage, and construing all reasonable inferences in the light most favorable to Plaintiffs, the Court finds that Plaintiffs sufficiently allege that Defendant intercepted the communications for a criminal or tortious purpose. See A.D. v. Aspen Dental Mgmt., Inc., No 24 C 1404, 2024 WL 4119153, at *3 (N.D. Ill. Sept. 9, 2024) (finding that the "plaintiffs[']' allegations [were] sufficient to invoke HIPAA for purposes of the ECPA's crime-tort exception" where they alleged the defendant used Google and Meta tools on its health portal to collect patient data, share the data with third parties and boost its own revenues).

To the extent that factual issues remain as to Defendant's intent behind allowing Google and Meta tools on its Web Properties, the Court finds these issues are more appropriately resolved at the summary judgment stage. In re Grp. Health Plan Litig., 709 F. Supp. 3d at 720 (finding the determination as to the defendant's actual purpose in intercepting communications was a "factual undertaking" better suited for after discovery).[2] Moreover, while Defendant's intent in disclosing the

[2] The Court recognizes that district courts have come to varying conclusions as to whether the crime-tort exception applies under similar facts. Contrast T.D. v. Piedmont Healthcare, Inc. (*T.D. II*), No. 23-CV-5416, 2024 WL 5284883, at *3–4 (N.D. Ga. Dec. 10, 2024) (refusing to vacate dismissal of the plaintiffs' ECPA claim on a motion for reconsideration and determining that the crime-tort exception did not apply) with W.W., 2025 WL 722892, at *7 (applying the crime-tort exception and refusing to dismiss the plaintiff's ECPA claim). Given the lack of guidance on these newly-emerging data privacy issues from the Eleventh Circuit Court of Appeals and the diverging opinions on these issues in this Circuit and others, the Court finds it appropriate to allow Plaintiffs'

information may have in part been to make money, "[l]egitimate objectives, like increasing revenue, do not shield a party from liability for crimes or torts committed in the process." R.S., 2025 WL 103488, at *7 (noting that, for example, the ECPA does not insulate a defendant from liability where the defendant intends to unlawfully intercept communications for the purpose of committing blackmail). Here, Plaintiffs sufficiently allege that Defendant intended to violate HIPAA when it intercepted patients' communications on the Web Properties. Thus, the Court finds that the crime-tort exception applies and, to the extent Defendant seeks dismissal of this claim, Defendant's Motion to Dismiss is **DENIED**.

CONCLUSION[3]

For the reasons set forth above, Defendant's Motion to Dismiss [Doc. 23] is **DENIED** insofar as Defendant seeks dismissal of Plaintiffs' claims for unjust

---

ECPA claim to move forward. See D.S. v. Tallahassee Mem'l HealthCare, No. 23cv540, 2024 WL 2318621, at *1 (May 22, 2024) (denying a defendant's motion to dismiss a plaintiff's ECPA claim based on similar facts and declining "to make dispositive merits determinations on a motion to dismiss, where the Rule 8 bar is law" and where the case concerned "complicated and novel legal issues").

[3] In a footnote on the final page of their response brief, Plaintiffs request leave to amend their complaint if the Court finds any of their claims subject to dismissal. [Doc. 27, p. 35 n.14]. Plaintiffs' request to amend was not made in the appropriate form, and the Court denies the request. See Davidson v. Maraj, 609 F. App'x 994, 1002 (11th Cir. 2015) ("It has long been established in this Circuit that a district court does not abuse its discretion by denying a general and cursory request for leave to amend contained in an opposition brief.").

enrichment (Count VII) and violation of the ECPA (Count VIII). However, the Motion is **GRANTED** insofar as it seeks dismissal of Plaintiffs' remaining claims.[4]

The parties are **HEREBY ORDERED** to file a Joint Preliminary Report and Discovery Plan, as required under Local Rule 16.2, no later than fourteen days from the date of this Order. The parties are notified that a failure to comply with this Order may result in sanctions, including dismissal. In the event that the parties do not file a Joint Preliminary Report and Discovery Plan, the Clerk is **DIRECTED** to submit the case at the expiration of the applicable time period.

SO ORDERED this 21st day of August, 2025.

J. P. BOULEE
United States District Judge

[4] In accordance with this Order, Plaintiffs' claim for invasion of privacy (Count I) is dismissed with prejudice, and the following claims are dismissed without prejudice: breach of fiduciary duty (Count II); negligence (Count III); negligence per se (Count IV); breach of implied contract (Count V); and breach of express contract (Count VI).