IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

EDWARD SWEAT, *et al*., individually and on behalf of a class of similarly situated individuals,	§	
	§	CIVIL ACTION NO. H-24-775
Plaintiffs,	§	
v.	§	
HOUSTON METHODIST HOSPITAL,	§	
Defendant.	§	

MEMORANDUM AND OPINION

Edward and Marie Sweat sued Houston Methodist Hospital, seeking to represent a class of individuals who had their personal health information disclosed by a tracking Pixel installed on Methodist's website. (Docket Entry No. 1-1). The court granted Methodist's motion to dismiss the state-law claim for invasion of privacy. (Docket Entry No. 28). The remaining claims allege that Methodist is liable for violating the Wiretap Act, 18 U.S.C. §§ 2510-2523, and for state-law unjust enrichment. (*Id.*). The parties conducted discovery. Methodist now moves for summary judgment on the remaining claims, arguing that its actions do not satisfy the Wiretap Act's crime-tort exception because it did not know that it was disclosing individually identifiable health information and because its only purpose in using the Pixel was to improve the effectiveness of its advertising and public health communications. (Docket Entry No. 52). The Sweats have responded to the motion, arguing that Methodist's acts in disclosing the information obtained by the Pixel are sufficient for liability. (Docket Entry No. 58).

Based on the pleadings, the motion and response, the record, and the applicable law, this court grants Methodist's motion for summary judgment. Final judgment is separately entered.

The reasons are set out below.

I. Background

Methodist is a nonprofit hospital serving the greater Houston area. (Docket Entry No. 52-6 at 8). To connect patients with doctors for medical care, its marketing department conducts community outreach, including advertising and public health campaigns. (*Id*. at 8–9). To track the performance of these outreach efforts, Methodist installed a Facebook tracking Pixel on public-facing pages of its website.[1] (*Id.* at 9; Docket Entry No. 52-10 at 8, 10). Methodist was hardly the only hospital to use the Pixel; fully one-third of the nation's top 100 hospitals did so. (Docket Entry No. 52-19 at 2). Methodist's stated purpose in implementing the Pixel was to learn if its outreach campaigns were accomplishing its goal of attracting people to its website and taking further "intent" actions, such as clicking a button on the site indicating that the person was going to schedule an appointment. (Docket Entry No. 52-6 at 9; Docket Entry No. 58-7 at 4, 5).

Methodist first implemented the Pixel in 2017, on the advice of Rise Interactive, a digital advertising agency. (Docket Entry No. 52-16). Methodist states that Rise Interactive advised the hospital that the Pixel was "safe" to use. (Docket Entry No. 52-11 at 8). Methodist later changed its advertising agency from Rise Interactive to Fathom SEO, a choice driven in part by Fathom's experience in healthcare marketing. (Docket Entry No. 52-10 at 12). Methodist states that Fathom also advised the hospital that the Pixel was safe to use. (Docket Entry No. 52-11 at 8). Fathom's agreement with Methodist stated that Fathom would provide services "in accordance with all applicable law, industry standards, and professional requirements." (Docket Entry No. 52-4).

---

[1] The parties generally—but not always—refer to "Facebook" instead of "Meta" when identifying the company that created the Pixel and received the sensitive information. (*See generally* Docket Entry Nos. 52, 58). In the first amended complaint, the Sweats stated that their information was improperly disclosed to "Meta Platforms, Inc. d/b/a Meta ("Facebook")." (Docket Entry No. 6 at 2). In line with the parties' use, the court generally refers to Facebook but refers to Meta when the underlying source (for example, a privacy policy or email chain) identifies the company as Meta.

As part of Fathom's services, Methodist received reports based on aggregated data gathered from the Pixel on the performance of its advertising and public health campaigns. (Docket Entry No. 52-9). The data provided Methodist with information, including the number of impressions on a social media post—the number of times its content was displayed on a user's screen, regardless of whether the user engaged with it or not—and the number of "lead actions" (such as scheduling an appointment) taken on Methodist's website in response to the advertised activity. (*Id.*). Methodist points to an example in one report showing that 2,078 users saw its "monthly reminder" on Facebook to schedule a mammogram and that 374 visited Methodist's website to do so. (Docket Entry No. 52 at 19) (citing Docket Entry No. 52-9). The aggregated data that Methodist received did not include information identifying the individuals who were seeking or obtaining healthcare services at Methodist. (Docket Entry No. 54-3). Methodist employees all testified that they believed that the Pixel data did not collect individually identifiable health information. (*See, e.g.*, Docket Entry No. 52-6 at 9; Docket Entry No. 52-8 at 16; Docket Entry No. 52-10 at 7). Methodist did not embed the Pixel within MyChart, the individual patient portal. (Docket Entry No. 52-8 at 17; Docket Entry No. 52-10 at 10; Docket Entry No. 58-3 at 4).

On May 18, 2022, a reporter from *The Markup*, a nonprofit newsroom covering the technology industry, emailed Methodist for comment about its use of the Pixel. (Docket Entry No. 52-18). The reporter explained that the *Markup* had conducted tests of the Pixel on Methodist's website and the websites of other hospitals, and that these tests showed that the Pixel was potentially capturing sensitive health information in violation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. §§ 1320d-1320d-9. (*Id.*). After receiving this email, Methodist promptly contacted Fathom for more information about how the Pixel's data filter worked. (Docket Entry No. 52-12). Fathom's privacy officer stated that the

Pixel captured IP addresses but that "[s]ince health information is filtered out, and all data is hashed and randomized (meaning it can no longer be used to identify an individual,) Meta isn't collecting" protected health information. (*Id.*). The privacy officer added that Meta's systems were designed to filter out sensitive health information and that such information was "not collected." (*Id.*).

On May 23, 2022, following its discussion with Fathom, Methodist reached out to Meta for more information about what information the Pixel filtered out and what data it collected. (Docket Entry No. 52-20). In response, Meta "delivered highly sanitized non-answers." (Docket Entry No. 52 at 13). Meta's responses emphasized that personally identifying information should be "hashed before transmission" and that healthcare organizations should be "especially mindful" to configure Meta's tools so as to not send personal health information. Meta also stated that it had a filtering mechanism to "prevent [potentially sensitive health-related data] from being ingested into our ads ranking and optimization systems," and that if Meta's filter detected such data, it would send an email alerting the organization of the issue. (Docket Entry No. 52-21 at 12–15). Meta could not confirm if it was receiving certain health information, such as the names of patients making appointments with particular doctors. (*Id.* at 12).

Just before the June 16, 2022, publication of *The Markup*'s article on hospitals' use of the Pixel, Methodist removed the Pixel from its website. (Docket Entry No. 52-19 at 6). Methodist told *The Markup* that it believed Facebook "uses tools to detect and reject any health information, providing a barrier that prevents passage of [protected health information]," but that it had elected to remove the Pixel "for now to be sure we are doing everything we can to protect our patients' privacy while we are evaluating." (*Id.*). That ended Methodist's use of the Pixel. (Docket Entry No. 52-8 at 13).

In 2024, the Sweats filed this putative class action in Texas state court, asserting claims for invasion of privacy, violations of the Wiretap Act, and unjust enrichment based on Methodist's use of the Pixel.[2] (Docket Entry No. 1-1). Methodist removed based on federal question jurisdiction. (Docket Entry No. 1). This court later granted in part and denied in part Methodist's motion to dismiss the Sweats' first amended complaint, dismissing the invasion of privacy claim with prejudice but allowing the claims for violation of the Wiretap Act and unjust enrichment to proceed. (Docket Entry No. 28 at 9). On February 19, 2025, the court granted Methodist's motion to bifurcate discovery between the threshold issue of liability and class discovery. (Docket Entry No. 47). Extensive discovery proceeded on the issue of liability. Methodist now moves for summary judgment on the Wiretap Act and unjust enrichment claims. (Docket Entry No. 52).

II. The Legal Standard

"Summary judgment is appropriate where 'the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.'" *Springboards to Educ., Inc. v. Pharr-San Juan-Alamo Indep. Sch. Dist.*, 33 F.4th 747, 749 (5th Cir. 2022) (quoting FED. R. CIV. P. 56(a)). "A fact is material if it 'might affect the outcome of the suit.'" *Thomas v. Tregre*, 913 F.3d 458, 462 (5th Cir. 2019), *as revised* (Jan. 25, 2019) (quoting *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986)). "A factual dispute is genuine 'if the evidence is such that a reasonable jury could return a verdict for the nonmoving party.'" *Id.* (quoting *Anderson*, 477 U.S. at 248). When considering a motion for summary judgment, the court "must consider all facts and evidence in the light most favorable to the nonmoving party"

[2] The Sweats also asserted a claim for breach of implied contract. (Docket Entry No. 1-1 at 42). This claim was not included in their first amended complaint. (Docket Entry No. 6).

and "must draw all reasonable inferences in favor of the nonmoving party." *Ion v. Chevron USA, Inc.*, 731 F.3d 379, 389 (5th Cir. 2013).

The moving party "always bears the initial responsibility of informing the district court of the basis for its motion" and pointing to record evidence demonstrating that there is no genuine dispute of material fact. *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986); *see also* FED. R. CIV. P. 56(c). "When 'the non-movant bears the burden of proof at trial,' a party moving for summary judgment 'may merely point to the absence of evidence and thereby shift to the non-movant the burden of demonstrating by competent summary judgment proof that there is a dispute of material fact warranting trial.'" *MDK Sociedad De Responsabilidad Limitada v. Proplant Inc.*, 25 F.4th 360, 368 (5th Cir. 2022) (alteration adopted) (quoting *Nola Spice Designs, L.L.C. v. Haydel Enterprises, Inc.*, 783 F.3d 527, 536 (5th Cir. 2015)).

"Once the moving party has initially shown that there is an absence of evidence to support the non-moving party's cause, the non-movant must come forward with specific facts showing a genuine factual issue for trial." *Houston v. Tex. Dep't of Agric.*, 17 F.4th 576, 581 (5th Cir. 2021) (quotation marks and quoting reference omitted). "[A] party cannot defeat summary judgment with conclusory allegations, unsubstantiated assertions, or only a scintilla of evidence." *Jones v. Gulf Coast Rest. Grp., Inc.*, 8 F.4th 363, 368 (5th Cir. 2021) (quotation marks and quoting reference omitted). Rather, the nonmovant "must identify specific evidence in the record and articulate the precise manner in which that evidence supports [its] claim." *Shah v. VHS San Antonio Partners, L.L.C.*, 985 F.3d 450, 453 (5th Cir. 2021) (alteration adopted) (quotation marks and quoting reference omitted).

The movant is entitled to judgment as a matter of law when "the nonmoving party has failed to make a sufficient showing on an essential element of [its] case with respect to which [it]

has the burden of proof." *Celotex Corp.*, 477 U.S. at 323. But "[i]f 'reasonable minds could differ' on 'the import of the evidence,' a court must deny the motion." *Sanchez v. Young County*, 956 F.3d 785, 791 (5th Cir. 2020) (quoting *Anderson*, 477 U.S. at 250).

III. Analysis

A. The Wiretap Act

A plaintiff pleads a prima facie case under the Wiretap Act, 18 U.S.C. §§ 2510-2523, by alleging facts "showing that the defendant "(1) intentionally (2) intercepted . . . (3) the contents of (4) an electronic communication, (5) using a device." *Brown v. Learfield Commc'ns., LLC*, No. 1:23-cv-00374, 2024 WL 3676709, at *3 (W.D. Tex. June 27, 2024) (quoting *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 135 (3d Cir. 2015)). One exception is § 2511(2)(d), which provides that ordinarily no cause of action will lie against a person who is a "party to the communication" unless "such 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." 18 U.S.C. § 2511(2)(d). This provision is often called the "crime-tort exception." *Brown*, 2024 WL 3676709, at *4. The critical issue on summary judgment—as opposed to the motion to dismiss stage—is whether there are disputed factual issues material to determining whether Methodist used the Pixel "for the purpose of committing any criminal or tortious act." As relevant here, under HIPAA, it is a crime to "knowingly . . . disclose[] individually identifiable health information." 42 U.S.C. § 1320d-6(a).

Methodist makes two arguments for why the crime-tort exception does not apply. First, it argues that that because the summary judgment evidence shows that it did not "knowingly" disclose individually identifiable health information, it "committed no crime that could subject it

to liability under the Wiretap Act."[3] (Docket Entry No. 52 at 17–18). Second, Methodist argues that because the evidence shows that its only purpose was to gather aggregate data for digital marketing, rather than to commit any crime or tort, it cannot be liable under the Act. (*Id.* at 26).

In response, the Sweats argue that the evidence shows a genuine factual dispute material to determining whether Methodist knew that the Pixel was disclosing individually identifiable health information to Facebook, in violation of HIPAA.[4] (Docket Entry No. 58 at 10–12, 14–16). The Sweats also appear to argue that disclosing individually identifiable health information for a commercial purpose—even without knowledge of the disclosure of such information—violates HIPAA, meaning that Methodist's commercial purpose is sufficient to trigger the crime-tort exception to the Wiretap Act and resulting liability. (*Id.* at 17).

Although the parties largely frame the inquiry as whether there is a triable fact issue necessary to determine whether Methodist violated HIPAA, the threshold issue is not whether Methodist violated HIPAA, but whether it acted with the *purpose* of violating HIPAA. "Under section 2511, 'the focus is not upon whether the interception itself violated another law; it is upon whether the *purpose* for the interception—its intended use—was criminal or tortious.'" *Sussman v. Am. Broadcasting Cos., Inc.*, 186 F.3d 1200, 1202 (9th Cir. 1999) (quoting *Payne v. Norwest*

---

[3] Methodist largely does argue that it did not disclose individually identifiable health information. (*See generally* Docket Entry Nos. 52, 62). While it asserts in passing that "[e]ven viewing Plaintiffs' evidence in the most favorable light, it is far from evident that the Pixel did routinely intercept" individually identifiable health information, it makes this argument only in a footnote. (Docket Entry No. 52 at 25 n.18). "[A]n argument raised in a footnote is insufficient and may be disregarded by the Court." *Gate Guard Servs. L.P. v. Perez*, 14 F. Supp. 3d 825, 833 (S.D. Tex. 2014).

[4] In their amended complaint, the Sweats alleged violations of HIPAA, two Texas state statutes, and invasion of privacy as the bases for liability under the crime-tort exception to the Wiretap Act. (Docket Entry No. 6 at 37). The court dismissed the invasion of privacy claim with prejudice, (Docket Entry No. 28), and in their response brief, the Sweats rely only on HIPAA as the basis for the crime-tort exception and do not mention the previously asserted Texas state statutes. (*See generally* Docket Entry No. 58). The court reviews only the alleged HIPAA violation as the basis for the crime-tort exception.

Corp., 911 F. Supp. 1299, 1304 (D. Mont. 1995), *aff'd in part and rev'd in part*, 113 F.3d 1079 (9th Cir. 1997)) (affirming summary judgment for the defendants because while ABC's taping of the plaintiffs "may well have been a tortious invasion of privacy under state law, plaintiffs have produced no probative evidence that ABC had an illegal or tortious purpose when it made the tape"); *see also Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010) ("Congress chose the word 'purpose' for a reason. Therefore, the offender must have as her objective a criminal or tortious result.'"); *Cohen v. Casper Sleep Inc.*, No. 17 Civ. 9325, 2018 WL 3392877, at *4 (S.D.N.Y. July 12, 2018) ("[Plaintiff] fails to demonstrate that Defendants' primary purpose was to commit a tort. Instead, he claims that Defendants' conduct amounted to a tort. But whether a tort was committed is irrelevant—the test is whether Defendants intended to commit a tort." (citation and emphasis omitted)).

Courts have taken two different approaches to the issue of "purpose" under the crime-tort exception. "Several circuits have determined that, to plead the crime-tort exception, the allegedly unlawful act must be independent of the allegedly unlawful interception." *See Brown*, 2024 WL 3676709, at *4. Some courts have dismissed similar HIPAA-based Wiretap Act cases on the ground that the alleged HIPAA violation was not independent of the interception itself.[5] *See, e.g.*,

[5] Methodist urges this court to find that, under the "independent act" approach, the crime-tort exception does not apply because the act of transmission is the same as the purported violation of HIPAA. (Docket Entry No. 52 at 23). Methodist points out that HIPAA does not allow a private right of action and that argues that "if the Wiretap Act becomes a back door to civil liability based on a purported HIPAA violation, then hospitals will be mired in the exact kind of private litigation that Congress meant to avoid." (*Id.* at 24). At least one court has stated that a plaintiff's "assertion of [a Wiretap Act] violation based on an alleged HIPAA violation may be reasonably viewed as an attempted end run around HIPAA's limitations to seek relief for the same alleged harm." *Roberts v. Charlotte Mecklenburg Hosp. Auth.*, No. 3:24-CV-00382, 2025 WL 880538, at *3 n.1 (W.D.N.C. Mar. 20, 2025), *appeal docketed* No. 25-1420 (4th Cir. Apr. 21, 2025). While there is merit to this argument, the court need not consider it because the summary judgment record evidence does not support an inference that Methodist acted with the necessary criminal or tortious purpose.

Doe v. Kaiser Found. Health Plan, Inc., No. 23-cv-02865, 2024 WL 1589982, at *10 (N.D. Cal. Apr. 11, 2024). Courts using the second, "primary purpose," approach "find that the crime-tort exception applies only where either the 'primary motivation' or 'determinative factor' in a party's interception was to commit a crime or tort.'" *Brown*, 2024 WL 3676709, at *4. Relying on this approach, some courts have dismissed similar HIPAA-based Wiretap Act cases because the defendant's primary motivation was to obtain a commercial advantage, not to commit a crime or a tort. *See, e.g.*, *Roe v. Amgen, Inc.*, No. 2:23-cv-07448, 2024 WL 2873482, at *6 (C.D. Cal. June 5, 2024). Courts also sometimes blend these approaches. *See, e.g.*, *Cooper v. Mount Sinai Health Sys., Inc.*, 742 F. Supp. 3d 369, 378–82 (S.D.N.Y. 2024) (applying both the independent act and primary purpose approaches). But to find liability under any of these approaches, the plaintiff must plead or, on summary judgment, present evidence raising a factual dispute as to whether the defendant intended to commit a crime or tort. *See, e.g.*, *Brown*, 2024 WL 3676709, at *5.

Taking the summary judgment evidence in the light most favorable to the non-moving parties, the summary judgment record shows that Methodist did not act with the "purpose of committing any criminal or tortious act" that would trigger the crime-tort exception to the Wiretap Act. First, there is no evidence that Methodist acted with the purpose of violating HIPAA by disclosing individually identifiable health information; the evidence shows that it did not know it was doing so. Second, the evidence shows that Methodist's only purpose was to improve its marketing and outreach, which is devoid of the intent to commit a crime or a tort and is therefore insufficient to allow the Sweats' claims to proceed under the crime-tort exception.

As to the first issue, Methodist received reports of aggregated information that did not show any individually identifiable data. Although these reports were based on interactions with arguably sensitive portions of Methodist's website, such as pages indicating if patients were going

to schedule appointments, the information collected was reported to Methodist only as collective, anonymous data. (Docket Entry No. 58-3 at 4). Houston Methodist's digital marketing director testified that Fathom, which ran the hospital's advertising campaigns, worked with other large healthcare systems "as to th[e] common practice" of using the Pixel, which is why she did not have a reason to look further into how the Pixel functioned. (Docket Entry No. 58-3 at 8). Her understanding is borne out by the fact that the one-third of the nation's top 100 hospitals used the Pixel during the relevant period. (Docket Entry No. 52-19 at 2).

Methodist employees uniformly testified that they did not believe that the Pixel was collecting or disseminating any individually identifiable health information. (Docket Entry No. 52-5 at 10; Docket Entry No. 52-6 at 9; Docket Entry No. 52-7 at 10; Docket Entry No. 52-8 at 16; Docket Entry No. 52-10 at 7). This testimony is supported by facts showing that, on learning of *The Markup*'s inquiry, Methodist immediately reached out to Fathom and Meta asking whether Meta was capturing personally identifiable health information and what filters it had in place to prevent it from receiving such information. (Docket Entry No. 52-14). Meta's own privacy policy at the time stated that "[i]f Meta's signals filtering mechanism detects Business Tools data that it categorizes as potentially sensitive health-related data, the filtering mechanism is designed to prevent that data from being ingested into our ads ranking and optimization systems." (Docket Entry No. 52-34 at 2). Methodist states that it never received a promised email from Meta alerting the hospital that Meta was receiving sensitive personal health information. (Docket Entry No. 62 at 4).

The Sweats argue that there is a genuine factual dispute material to determining Methodist's knowledge because: (1) aggregate data can only be created from individual data; (2) Methodist's privacy policy and Facebook's filter disclosure "make[] clear" that the hospital knew

that it was sending Facebook sensitive data; and (3) Methodist "failed to take basic measures to ensure that it was not disclosing" protected health information. (Docket Entry No. 58). These assertions all fail to show that there is a triable issue as to whether Methodist knowingly disclosed—or was willfully blind to its disclosure of—protected health information.[6] Instead, these assertions essentially accuse Methodist of being negligent in its use of the Pixel, which is clearly insufficient to show that Methodist acted with the purpose of violating HIPAA.

First, aggregate data can be created from individual data that is anonymized at the input level. The fact that Methodist received reports showing aggregate data does not raise an inference that Methodist knew that it was collecting and disclosing individually identifiable personal health information. No Methodist employee understood the reports to be based on protected health information. Although the Sweats argue that the employees' credibility is a matter for the jury, (Docket Entry No. 58 at 22), the Sweats have not presented or pointed to any summary judgment evidence contravening the employees' consistent testimony. *See In re Pharmatrak, Inc. Privacy Litig.*, 292 F. Supp. 2d 263, 268 (D. Mass. 2003) (granting summary judgment to the defendants in part because Pharmatrak's chief of technology testified that the company did not intend to collect sensitive information, that he did not know it was doing so, and the plaintiffs "offer[ed] no evidence to contradict these statements"). Second, the Sweats' single-sentence excerpt from Methodist's privacy policy does not demonstrate that Methodist must have known it was sending individually identifiable health information to Facebook.[7] Third, the wording of the filter

---

[6] Willful blindness requires that a defendant have a subjective awareness of a high probability of the existence of illegal conduct and purposefully contrived to avoid learning of that conduct. *See United States v. Lee*, 966 F.3d 310, 234 (5th Cir. 2020).

[7] As Methodist points out, the Sweats excerpt a single sentence from a section of the privacy policy on "Advertisements." (Docket Entry No. 62 at 3). The thorough section of the privacy policy on "Shar[ing] Information with Third Parties" states that Methodist shared "non-Personal Information, such as aggregated

disclosure—which does not make clear how, when, or other details as to whether Facebook's filter rejected sensitive health data—at most supports an inference that Methodist should have looked more closely at the filter's functioning. But Methodist's arguable negligence is insufficient to raise a genuine factual dispute as to whether it acted with the purpose of violating HIPAA. *See In re Doubleclick Inc. Priv. Litig*, 154 F. Supp. 2d 497, 515 (S.D.N.Y. 2001) (concluding that "the legislative record suggests that the element of 'tortious' or 'criminal' *mens rea* is required to establish a prohibited purpose under § 2511(2)(d)").

The uncontroverted summary judgment evidence is that Methodist used the information received from its use of the Pixel only for the purpose of improving its marketing and outreach. (Docket Entry No. 52-6 at 9; Docket Entry No. 52-7 at 5; Docket Entry No. 52-10 at 8). Although the Fifth Circuit has not yet ruled on the disputed question of whether the crime-tort exception applies when a medical provider's primary purpose in disclosing information is commercial, (*see* Docket Entry No. 28 at 8), the court need not reach this question because a commercial purpose must still be tethered to a criminal or tortious purpose. As detailed above, the record does not show that Methodist acted with the purpose of violating HIPAA. Even the cases the Sweats cite emphasize that there must be an unlawful purpose in addition to a lawful purpose to trigger the crime-tort exception in cases in which there may be dual motives. (Docket Entry No. 58 at 21); *see Lugo v. Inova Health Care Servs.*, No. 1:24-cv-700, 2025 WL 905191, at *8 (E.D. Va. Mar. 25, 2025) (denying a motion to dismiss because "many crimes and torts are committed for financial

---

user statistics, with third parties" but that it "d[id] not share your Personal Information that we have collected directly from you on our Service with third parties for those third parties' direct marketing purposes unless we have given you the choice to consent or withhold consent." (Docket Entry No. 52-17 at 3). The policy adds that "[i]f we de-identity data about you, it is not treated as Personal Information by us, and we may share it with others freely." (*Id.*). The Sweats' single excerpted line from a different section of the policy does not demonstrate a genuine issue of material fact as to whether Methodist knew it was disclosing individually identifiable health information.

gain. Therefore, having a commercial purpose in addition to the purpose of violating HIPAA or [a state privacy law] does not immunize INOVA from Plaintiff's [Wiretap Act] claims"); *Cooper*, 742 F. Supp. 3d at 378 (stating that "the mere existence of a lawful purpose alone does not sanitize an interception that was also made for an illegitimate purpose" (citation modified)).

The Sweats seemingly attempt to avoid the issue that a commercial purpose alone cannot suffice by arguing that "the fact that [Methodist], as admitted to in its own Motion, implemented the Meta Pixel for a 'commercial advantage' of operating its marketing campaigns, is itself evidence that [Methodist] intentionally violated HIPAA." (Docket Entry No. 58 at 6). That is, the Sweats argue that Methodist's commercial purpose is sufficient to trigger the crime-tort exception because HIPAA makes disclosing information for a "commercial advantage" unlawful. (*See also id.* at 17, 21–22). But this misconstrues HIPAA. The statute does not criminalize the mere disclosure of protected information with the intent to use that information for commercial advantage. Rather, HIPAA states that a person is criminally liable for "knowingly . . . disclos[ing] individually identifiable health information" and then increases the penalties if the offense was committed with intent to use the information "for commercial advantage" or "personal gain." 42 U.S.C. § 1320d-6 (a)(3), (b)(3). The disclosure of what was not known to be personally identifiable health information, but instead believed to be aggregate data, for a commercial purpose, is not a crime or a tort. It cannot trigger the crime-tort exception, which requires the purpose of committing a criminal or tortious "act." 18 U.S.C. § 2511(2)(d).

"Section 2511(2)(d)'s legislative history and caselaw make clear that the 'criminal' or 'tortious' purpose requirement is to be construed narrowly, covering only acts accompanied by a specific contemporary intention to commit a crime or tort." *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. at 515. Taking the evidence in the light most favorable to the Sweats, they have not

met their burden of showing that Methodist had a contemporaneous intent to commit a crime or a tort. Summary judgment is granted to Methodist on the Sweats' Wiretap Act claim.

B. Unjust Enrichment

The Sweats do not dispute that Methodist did not sell the individually identifiable health information it collected for profit and so have dropped their claim for unjust enrichment. (Docket Entry No. 58 at 6 n.1). Summary judgment is granted to Methodist on this claim as well.

IV. Conclusion

Courts have long recognized the importance of privacy in the context of health information. *See, e.g.*, *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 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 or genetic make-up.").[8] Methodist's use of the Pixel is a good example of the careful line hospitals must draw between efforts to raise money and promote public health awareness on the one hand and the importance of maintaining privacy for those who seek or obtain medical care on the other. The summary judgment evidence demonstrates that Methodist did not use the Pixel with the purpose of committing a crime or a tort. There is no basis for liability under

[8] In addition to the splintered approaches to the crime-tort exception in the context of HIPAA discussed above, courts have also had difficulty determining what kinds of pleading allegations suffice to show that a defendant disclosed individually identifiable health information in violation of HIPAA. *See, e.g. Castillo v. Costco Wholesale Corp.*, No. 2:23-cv-01548, 2024 WL 4785136, at *6–*7 (W.D. Wash. Nov. 14, 2024). Moreover, the question of what constitutes individually identifiable health information has gotten even more complicated with the recent decision in *Am. Hospital Ass'n v. Becerra* vacating a guidance from the Department of Health and Human Services adding to the term's definition. 738 F. Supp. 3d 780, 803 (N.D. Tex. 2024). The treacherous terrain is even further evidenced by the recent access given to the Department of Government Efficiency to Social Security information, which includes health information. *See Soc. Sec. Admin. v. Am. Fed'n of State, Cnty., and Mun. Emps.*, 605 U.S. ----, 145 S. Ct. 1626 (2025) (reversing an en banc Fourth Circuit Court of Appeals ruling that had enjoined the Social Security Administration from granting Department of Government Efficiency personnel access to certain personally identifiable information).

the crime-tort exception to the Wiretap Act. Summary judgment for Methodist is granted. Final judgment is entered by separate order.

SIGNED on September 22, 2025, at Houston, Texas.

Lee H. Rosenthal
Senior United States District Judge