IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

JANE DOE, Individually and on behalf of all others similarly situated, **Plaintiff,** **v.** **DEACONESS ILLINOIS UNION COUNTY HOSPITAL, INC., d/b/a DEACONESS ILLINOIS UNION COUNTY, d/b/a UNION COUNTY HOSPITAL,** **Defendant.**	**Case No. 3:24-CV-02284-NJR**

MEMORANDUM AND ORDER

ROSENSTENGEL, Chief Judge:

This case arises out of Defendant Deaconess Illinois Union County Hospital's use of tracking tools on its website, which allegedly caused protected health information ("PHI") and personally identifying information ("PII") to be transmitted to unauthorized third parties, including Meta Platforms, Inc. ("Meta"), Google, LLC ("Google"), DoubleClick Ads, and Microsoft Corp. ("Microsoft") (collectively the "Third Parties"). Plaintiff Jane Doe brought this putative class action on behalf of herself, and others whose PHI and PII were allegedly compromised. Doe advances claims of (i) negligence; (II) negligence *per se*; (i) invasion of privacy—intrusion upon seclusion; (iv) breach of express contract; (v) breach of implied contract; (vi) unjust enrichment; (vii) breach of bailment; (viii) violation of the Illinois Eavesdropping Statute, 720 ILCS 5/14, *et seq.*; (ix) violation of the Electronic Communications Privacy Act ("ECPA" or "Wiretap Act"),

18 U.S.C. §§ 2511(1), *et seq.*; (x) violation of the ECPA, 18 U.S.C. § 2511(3)(a) ("unauthorized divulgence"); (xi) violation of the Stored Communications Act ("SCA"), 18 U.S.C. § 2701, *et seq.*; and (xii) violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq.* Deaconess has moved to dismiss the case pursuant to Federal Rule of Civil Procedure 12(b)(6). (Doc. 22).

BACKGROUND

Deaconess is a 25-bed hospital in Anna, Illinois, which provides "complete inpatient and outpatient care including emergency, medical and surgical services." (Compl., Doc. 1 ¶ 39). Like most hospitals today, Deaconess maintains a website (www.unioncountyhospital.com) that allows patients to manage their care by, for instance, obtaining test results, scheduling appointments, paying bills, and researching providers. (*Id.* ¶¶ 10-11). The website also provides information about Deaconess's providers and services to the general public. (*Id.* ¶ 10).

The website is equipped with "code-based tracking devices known as 'trackers' or 'tracking technologies,'" that allegedly "collect[] and transmit[] patients' [p]rivate information" to the Third Parties. (*Id.* ¶ 10). The complaint explains a "tracker" as follows:

> A tracker . . . is a snippet of code embedded into a website that tracks information about its visitors and their website interactions. When a person visits a website with an [sic] tracker, it tracks "events" (i.e., user interactions with the site), such as pages viewed, buttons clicked, and information submitted. Then, the tracker transmits the event information back to the website server and to third parties, where it can be combined with other data and used for marketing. (*Id.* ¶ 14).

One example of such a tracker is Meta's "Pixel," which tracks a visitor's activity on the Deaconess website, including their search terms, button clicks, and form

submissions. (*Id.* ¶ 15). The Meta Pixel also allows the visitor's website interactions to be linked to their Facebook ID, so that otherwise anonymized data can be matched to a specific individual. (*Id.*). Doe alleges that "[b]y installing the Meta Pixel on its [w]ebsite, [Deaconess] effectively planted a bug on [her and the class members'] web browsers and compelled them to disclose" PHI and other sensitive information to Meta without their knowledge and consent. (*Id.* ¶ 16). Deaconess allegedly "utilized data from these trackers to market their services and bolster their profits." (*Id.* ¶ 20). Meta, in turn, "utilizes data from the Meta Pixel . . . to build data profiles for the purpose of creating targeted online advertisements and enhanced marketing services, which it sells to additional third parties for profit." (*Id.*). Deaconess allegedly also installed other trackers like "Google Analytics, Google Tag Manager . . ., Double Click Ads, and Microsoft's Azure Monitor Application Insights, which operate similarly to the Meta Pixel." (*Id.* ¶ 23).

Doe and the absent class members (collectively the "Class") are current and former patients of Deaconess who visited the website in connection with their healthcare. (*Id.* ¶¶ 12, 247, 248). Unbeknownst to them, Deaconess embedded trackers from the Third Parties into its website, which "surreptitiously forc[ed]" the Class "to transmit intimate details about their medical treatment" to the Third Parties without their consent. (*Id.* ¶ 13).

How it Works: Capture and Disclosure of PHI and PII

When a person visits a website, their web browser sends an HTTP (Hypertext Transfer Protocol) request to a server asking it to retrieve certain information. (*Id.* ¶ 63). The server then sends an HTTP response that contains the requested information in the

form of pages, images, words, and buttons (known as "Markup") to be displayed on the visitor's screen. (*Id.*). Every website consists of Markup and source code. (*Id.* ¶ 64). Source code is "a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code." (*Id.*). Source code can thus command a user's web browser to send certain information to third parties without their knowledge or consent. (*Id.* ¶ 65).

Doe has used Deaconess's website to search for physicians and treatment information, pay for medical services, and access the "Patient Portal," a private account containing her PHI and PII. (*Id.* ¶ 176). She has also been a Facebook user since 2007 and "began receiving medical advertisements in her Facebook feed regarding the medical conditions and symptoms she searched for and viewed" on the website. (*Id.* ¶ 177). This happened because Deaconess, through its utilization of trackers, allegedly captured and disclosed, among other things, (i) each instance in which she visited its homepage (*Id.* ¶ 121), (ii) her search activities on the Deaconess website, including her requests to enter the patient portal (*Id.* ¶ 123), (iii) each instance in which she navigated to the website's "Services" page to research medical treatments (*Id.* ¶ 129), (iv) specific searches for services, for instance, by visiting a page titled "Emergency Room – Union County Hospital" (*Id.* ¶ 133), (v) and each search for specific providers (*Id.* ¶ 137). The mechanics of this process can be explained by way of an example in which a patient searches for a specific provider: "if a patient clicked to learn more about Dr. Courtney Y. Ledbetter, [Deaconess] sent a SubscribedButtonClick event to [Meta], revealing that the patient clicked to "VIEW MORE" about "provider/courtney-y-ledbetter." (*Id.* ¶ 140). Thus,

discrete online activity events, including those in which visitors searched for treatments and providers to address their health concerns, were reported to the Third Parties after the trackers captured them.

Doe relied on Deaconess's promises to keep her PHI and PII secure and not share it with third parties. Because these promises were allegedly broken, Doe suffered a range of injuries including a loss of privacy, overpayment for services from Deaconess, an inability to share in the profits and savings derived from Deaconess's improper capture and disclosure of PHI and PII, emotional distress, decreased value of her private information, lost benefit of the bargain, increased risk of future harm due to the disclosure of her PHI and PII, and statutory damages. (*Id.* ¶ 185).

Doe filed a putative class action complaint in this Court in October 2024. (Doc. 1). She seeks to represent a nationwide class of Plaintiffs consisting of:

> All patients of [Deaconess] whose Private Information was disclosed by [Deaconess] to third parties through the Meta Pixel and related technology without authorization. (*Id.* ¶ 247).

Doe also seeks to represent an Illinois subclass, which she defines as:

> All patients of [Deaconess] who are Illinois citizens and whose Private Information was disclosed by [Deaconess] to third parties through the Meta Pixel and related technology without authorization. (*Id.* ¶ 248).

LEGAL STANDARD

A motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) "tests whether the complaint states a claim on which relief may be granted." *Richards v. Mitcheff*, 696 F.3d 635, 637 (7th Cir. 2012). The Court accepts as true the complaint's well-pleaded factual

allegations and draws all reasonable inferences in the plaintiff's favor. *Burke v. 401 N. Wabash Venture, LLC*, 714 F.3d 501, 504 (7th Cir. 2013).

To survive a Rule 12(b)(6) motion, a plaintiff only needs to allege enough facts to state a claim for relief that is plausible on its face. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "Plausibility does not mean probability: a court reviewing a 12(b)(6) motion must 'ask itself *could* these things have happened, not *did* they happen.'" *Huri v. Off. of the Chief Judge of the Cir. Ct. of Cook Cnty.*, 804 F.3d 826, 833 (7th Cir. 2015) (quoting *Swanson v. Citibank, N.A.*, 614 F.3d 400, 404 (7th Cir. 2010)). "A claim is plausible where a plaintiff 'pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.'" *Bilek v. Fed. Ins. Co.*, 8 F.4th 581, 586 (7th Cir. 2021) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). This means that the plaintiff must offer "some specific facts to support the legal claims asserted in the complaint." *Id.* (quoting *McAuley v. City of Chicago*, 671 F.3d 611, 616 (7th Cir. 2011) (citation modified)).

DISCUSSION

Deaconess has moved to dismiss this action in its entirety. The Court thus addresses the viability of each of Doe's 12 claims in turn.

Negligence and Contract-based Claims (Counts I, II, IV, and V)

Deaconess's first argument concerns Doe's claims of negligence (Count I), negligence *per se* (Count II), breach of express contract (Count IV), and breach of implied contract (Count V). According to Deaconess, Doe failed to present viable claims under these theories because she has not alleged "actual damages" to support them. Although the Court partially agrees with Deaconess, its attempt to broadly attack these claims

based on the lack of "actual damages" overlooks some important nuance.

a. Contract Claims

"Illinois law is clear that, to state a claim for breach of contract, one must be able to prove actual damage." *TAS Distr. Co. v. Cummings Eng. Co.*, 491 F.3d 625, 631 n.6 (7th Cir. 2007). "Merely showing that a contract has been breached without demonstrating actual damage does not suffice." *Id.* at 631. Actual damages are damages of a pecuniary nature; emotional, reputational, and other non-quantifiable damages are insufficient. *Stevens v. McGuireWoods LLP*, 43 N.E.3d 923, 927 (Ill. 2015); *In re Estate of Powell*, 12 N.E.3d 14, 20 (Ill. 2014); *Imperial Apparel Ltd. v. Cosmo's Des. Direct., Inc.*, 882 N.E.2d 1011, 1018 (Ill. 2008); *Flores v. Aon Corp.*, 242 N.E.3d 340, 356 (Ill. App. Ct. 2023) ("To successfully make a breach of implied contract claim, a plaintiff must allege actual monetary damages."); *accord Petta v. Christie Bus. Hold. Co.*, 230 N.E.3d 162, 169 (Ill. App. Ct. 2023). Here, Doe claims that she and the Class sustained a "decreased value of their private information, emotional harm, loss of privacy, the [loss of] revenues, profits, and savings attributable to [Deaconess's] unauthorized sale of Plaintiffs' Private Information, and increased risk of future harm." (Pl. Resp. to Mot. to Dismiss, (Doc. 24, p. 12)).

These damages do not support a breach of contract claim. Emotional damages, the risk of future harm, and the loss of privacy are non-starters because they are, by definition, not pecuniary in nature. *M.C. v. E. Side Health Dist.*, No. 3:24-CV-01336, 2025 WL 435992, at *4 (S.D. Ill. Feb. 7, 2025). The alleged diminution in the value of Doe's personal information, moreover, cannot sustain a contract action because it is entirely speculative. *Flores*, 242 N.E.3d at 356; *Petta*, 230 N.E.3d at 169. Beyond that, the Illinois

Appellate Court has questioned whether a person even holds a property right in her personal information. *See id.* ("This court is unaware of any case law holding that a person has a property right in her personal information."). It should come as no surprise, then, that this Court is disinclined to recognize a damages theory based on a right that apparently does not exist under Illinois law. Finally, the lost revenues and profits attributable to Deaconess's alleged disclosure of Doe's personal information are insufficient because Doe, by her own admission, had a contract with Deaconess to receive healthcare; she did not enter into a profit-sharing agreement whereby Deaconess would market and sell her personal information. To accept lost revenues and profits as cognizable damages in support of her breach of contract claim would be to invent a new contract altogether. *Dinerstein v. Google, LLC*, 484 F. Supp. 3d 561, 592 (N.D. Ill. 2020) (rejecting similar claim for "royalties" under breach of contract theory); *cf. Kurowski v. Rush Sys. for Health*, 683 F. Supp. 836, 845-46 (N.D. Ill. 2023) (*Kurowski II*) (similar damages did not satisfy "actual damages" requirement).

For these reasons, the Court finds that Doe has failed to allege actual damages that can support her breach of express contract and breach of implied contract claims (Counts IV and V respectively). These claims will accordingly be dismissed.

b. Negligence Claims

Deaconess appears to rely on the same argument concerning actual damages to contend that their omission from the complaint also renders Doe's negligence and negligence *per se* claims (Counts I and II respectively) deficient. These claims, however, are subject to a different damages inquiry.

In Illinois, a negligence claim can be based on one's emotional damages. *M.C.*, 2025 WL 435992, at *4; *see also In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 587 (N.D. Ill. 2022) ("There can be no dispute that Plaintiffs have alleged present injuries or damages; for instance, all allege experiencing emotional harms such as anxiety and increased concerns for the loss of privacy. . . . These types of non-economic damages are recoverable under Illinois law" in a negligence action); *Volling v. Antioch Rescue Squad*, 999 F.Supp.2d 991, 999 (N.D. Ill. 2013). Doe alleges that she and the Class suffered "the unauthorized access of [their] Private Information by third parties, the improper disclosure of their Private Information, lost benefit of their bargain, and lost value of their Private Information," (Doc. 24, p. 11-12), as well as "embarrassment, humiliation, frustration, and emotional distress." (Doc. 1 ¶ 287). These damages are cognizable in a negligence action, and Deaconess has offered no authority to the contrary. *See e.g.*, *Hannant v. Culbertson*, No. 4:24-cv-04164, 2025 WL 2413894, at *12 (C.D. Ill. Aug. 20, 2025); *Smith v. Loyola Univ. Med. Ctr.*, No. 23 CV 15828, 2024 WL 3338941, at *7 (N.D. Ill. July 9, 2024) ("Allegations of emotional harm, such as these, are sufficient to state a negligence claim under Illinois law, including in the data privacy context."). The Court thus finds that Doe has pled cognizable damages with respect to Counts I and II.[1]

[1] In Illinois, "[a] violation of a statute only constitutes negligence *per se* (which would mean strict liability) if the legislature clearly intends for the act to impose strict liability." *Flores*, 242 N.E.3d at 355. Although Doe links her negligence *per se* claim to violations of HIPAA and its associated regulations, she has not identified HIPAA, or any other statute or regulation, as a strict liability standard that would support such a claim. The Court is thus skeptical of the viability of Count II as currently pled. Count II nevertheless survives Deaconess's motion to dismiss at this stage because Deaconess has not raised the lack of a strict liability standard as a basis for dismissal. *See Hannant*, 2025 WL 2413894, at *14 ("Because Plaintiff makes no attempt to argue that the sources of law which she identified were intended to impose strict liability, the Court construes [her negligence *per se* claim] as another negligence claim that is based on violation of a statute.").

Invasion of Privacy – Intrusion upon Seclusion (Count III)

Doe's invasion of privacy – intrusion upon seclusion claim is based on her allegation that "she had a reasonable expectation of privacy in communicating her sensitive Private Information to Defendant—her medical provider—on its website, and Defendant utilized secret trackers to surreptitiously disclose that Private Information to unauthorized third parties without [her] consent." (Doc. 24, p. 13). Deaconess contends that this theory fails to offer an essential ingredient of an invasion of privacy claim based on intrusion upon seclusion: an intrusion. The Court agrees.

The Northern District of Illinois addressed a nearly identical invasion of privacy claim based on intrusion upon seclusion in *Kurowski v. Rush Sys. for Health*, 659 F. Supp. 3d 931, 943-44 (N.D. Ill. 2023) (*Kurowski I*). There, the plaintiff alleged that Rush (a healthcare provider), embedded source code on its website and its "MyChart" patient portal, which caused her private information to be captured and transmitted to Meta, Google, and others. *Id.* at 934. In addressing the plaintiff's invasion of privacy claim, Judge Kennelly focused on the "core" of her allegations, which was the defendant's "deployment of third-party source code that causes the transmission of patient data" to third parties. *Id.* at 943. These allegations, Judge Kennelly found, could not satisfy the "intrusion" element of an invasion of privacy claim because "the Illinois Supreme Court has explained that the core of this tort is the offensive prying into the private domain of another and that the basis of the tort is not publication of publicity." *Id.* (quoting *Dinerstein*, 484 F. Supp. 3d at 594 (alterations and quotation marks omitted)). Thus, "disclosures of private personal information do not support a claim for unauthorized

intrusion." *Dinerstein*, 484 F. Supp. 3d at 594. And while the plaintiff may have sufficiently alleged that *third parties* invaded her privacy, their liability, if any, was not imputed to the defendant. *Kurowski I*, 659 F. Supp. 3d at 944.

This Court finds *Kurowski I*'s reasoning, and the authorities it relied on, persuasive. Doe's allegations here are nearly identical to those offered in *Kurowski I*. She claims that Deaconess improperly captured and disclosed her PHI and PII as she utilized its website and patient portal. Nowhere has she alleged that Deaconess surreptitiously intruded into a private domain (whether physically or virtually) where it had no business being. *See Dinerstein*, 484 F. Supp. 3d at 594 ("Examples of such 'offensive prying' are 'invading someone's home; an illegal search of someone's shopping bag in a store; eavesdropping by wiretapping; peering into the windows of a private home; and persistent and unwanted telephone calls.'") (citation omitted). Indeed, Deaconess was the *intended recipient* of the information in question. Doe's theory, moreover, requires the Court to equate an improper *disclosure* of her private information with an *intrusion* into her private space. This would conflate two distinct forms of conduct and potentially expand the invasion of privacy tort beyond its recognized reach. The Court is not inclined to adopt such an unusual position, especially in light of the well-reasoned decisions from other district courts in Illinois that rejected similar arguments from plaintiffs on this point.

For this reason, Doe's invasion of privacy claim based on intrusion upon seclusion (Count III) will be dismissed.

Unjust Enrichment (Count VI)

The Court can make "short work" of Doe's unjust enrichment claim because

"[u]njust enrichment is not a separate cause of action under Illinois law." *Horist v. Sudler*, 941 F.3d 274, 281 (7th Cir. 2019). "Unjust enrichment is a common-law theory of recovery or restitution that arises when the defendant is retaining a benefit to the plaintiff's detriment, and this retention is unjust." *Cleary v. Philip Morris, Inc.*, 656 F.3d 511, 517 (7th Cir. 2011). "What makes the retention of the benefit unjust is often due to some improper conduct by the defendant. And usually[,] this improper conduct will form the basis of another claim against the defendant in tort, contract, or statute." *Id.* These observations from the Seventh Circuit are binding on this Court. They also make logical sense here.

Doe alleges that she was injured by Deaconess's improper capture and disclosure of her PHI and PII. Her unjust enrichment claim and 11 other statutory and common law claims assign liability based on this conduct. The unjust enrichment claim thus "rests on the same improper conduct alleged in another claim" and "will stand or fall with the related claim." *Id.* This means that, under Illinois law as interpreted by the Seventh Circuit, Doe cannot advance an unjust enrichment claim as a standalone action. *See Alliance Acceptance Co. v. Yale Ins. Agency*, 648 N.E.2d 971, 977 (Ill. App. Ct. 1995) ("The term 'unjust enrichment' is not descriptive of conduct that, standing alone, will justify an action for recovery") (quoting *Charles Hester Enterpr., Inc. v. Ill. Founders Ins. Co.*, 484 N.E.2d 349, 354 (Ill. App. Ct. 1985)); *accord Hannant*, 2025 WL 2413894, at *17 (dismissing unjust enrichment claim because it hinged on viability of other claims).

For this reason, Doe's unjust enrichment claim in Count VI will be dismissed.

Bailment (Count VII)

In Count VII, Doe asserts a claim of bailment under Illinois law. "A bailment is

'the delivery of goods for some purpose, upon a contract, express or implied, that after the purpose has been fulfilled they shall be redelivered to the bailor, or otherwise dealt with according to his directions, or kept till he reclaims them.'" *Kirby v. Chicago City Bank & Tr. Co.*, 403 N.E.2d 720, 723 (Ill. App. Ct. 1980) (quoting *Knapp, Stout & Co. v. McCaffrey*, 52 N.E. 898, 899 (Ill. 1899)). "Among the necessary elements of a bailment are an agreement by the bailor to transfer or deliver and the bailee to accept exclusive possession of goods for a specified purpose, the actual delivery or transfer of exclusive possession of the property of the bailor to the bailee, and acceptance of exclusive possession by the bailee." *Id.* Doe's bailment claim is based on her allegation that "she, the Class, and [Deaconess] contemplated a mutual benefit bailment when Plaintiff and Class members transmitted their Private Information to Defendant solely for purposes of receiving medical treatment and the payment thereof." (Doc. 24, p. 15-16). Deaconess then allegedly "breached that bailment by using, and Disclosing, Plaintiff's and the Class's Private Information for a different purpose than the Plaintiff and the Class intended, *i.e.* for marketing purposes instead of to facilitate their medical treatment, and for a longer time period and/or in a different manner or place than the parties intended." (*Id.*, p. 16). Deaconess contends that Doe fails to state a claim for bailment because it never received "exclusive possession" of the information in question. The Court agrees.

In *In re Mondelez Data Breach Litig.*, No. 23 C 3999, 2024 WL 2817489, at *9 (N.D. Ill. June 3, 2024), the court rejected a bailment claim based on the alleged exposure of the plaintiff's personal information, which arose out of a data breach at the plaintiff's law firm. The court observed that "[t]he law of bailment in Illinois does not map onto the

circumstances of this case, as no one can have "exclusive possession" of another person's personal information." *Id.* Neither the Illinois Supreme Court nor any lower state court had endorsed this type of bailment theory, and the *Mondelez* court was reluctant to be the first. *Id.*

This Court is similarly skeptical that the Illinois Supreme Court would recognize Doe's bailment theory. Doe's personal information was in at least two places at once when she shared it with Deaconess. By definition, then, no one had "exclusive possession" of it. *Id.* This logic is fatal to Doe's bailment claim and the authority she cites does little to refute it.

For instance, Doe relies on *Wright v. Autohaus Fortense, Inc.*, 472 N.E.2d 593, 594-95 (Ill. App. Ct. 1984), where the plaintiff left his car in a parking lot overnight and the defendant (an auto repair shop) arranged for a towing service to bring it the shop for repairs. The court concluded that once the car arrived at the repair shop, the defendant had "exclusive possession" of it. *Id.* at 595. This, in turn, created a bailment, even though the plaintiff retained a set of keys to the car. *Id.* at 595. It did not matter that the plaintiff could have used his spare keys to retrieve the car at any time because unless and until he did so, no one other than the defendant had possession of it. *Id.*

Doe relies on *Wright* for the proposition that a bailment was created even though she retained her own PHI and PII after sharing it with Deaconess, like the plaintiff who retained his car keys in *Wright*. This analogy is unpersuasive because exclusive possession of a car is not the same as exclusive possession of another person's personal information, which, as noted, can be possessed by more than one person after it is shared.

If anything, Doe's reliance on *Wright* validates the Court's skepticism about the viability of a bailment claim based on personal information. It is one thing to conclude that a car repair shop had "exclusive possession" of a car, even though the owner kept possession of a key to the car. It is quite another to extend that logic to the electronic transfer of personal information, where that information is captured by the intended recipient but also retained by the sender. The Court thus declines to adopt Doe's bailment theory. *See Todd v. Societe Bic, S.A.*, 21 F.3d 1402, 1412 (7th Cir. 1994) ("When given a choice between an interpretation of Illinois law which reasonably restricts liability, and one which greatly expands liability, [federal courts] should choose the narrower and more reasonable path (at least until the Illinois Supreme Court tells us differently).").

For this reason, Count VII of the complaint asserting a claim of bailment will be dismissed.

Violation of the Illinois Eavesdropping Statute (Count VIII)

In Count VIII, Doe asserts a claim under the Illinois Eavesdropping Statute, 720 ILCS 5/14, *et seq.* ("IES"). Curiously, Doe has not responded to Deaconess's arguments concerning her IES claim. The Court will nevertheless examine its viability to determine whether it survives Deaconess's motion.

720 ILCS 5/14-2(a)(2) makes it unlawful for a person to "knowingly and intentionally" "[u]se[] an eavesdropping device, in a surreptitious manner, for the purpose of transmitting or recording all or any part of any private conversation to which he or she is a party unless he or she does so with the consent of all other parties to the private conversation." 720 ILCS 5/14-2(a)(2). Deaconess argues that Doe cannot rely on

section 14-2(a)(2) to assert an IES claim because it applies only to "private conversations," which are defined as "any *oral communication* between 2 or more persons." *Id.* § 5/14-1(d) (emphasis added). The Court agrees with Deaconess that Doe's IES claim cannot proceed under section 14-2(a)(2) because she has not alleged the capture or interception of an "oral communication."

But the IES does not stop there. Section 5/14-2(a)(5) prohibits a person from "knowingly and intentionally" "[u]s[ing] or disclos[ing] any information which he or she knows or reasonably should know was obtained from a private conversation *or private electronic communication* in violation of [the IES], unless he or she does so with the consent of all of the parties." *Id.* § 5/14-2(a)(5) (emphasis added). A "private electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation." *Id.* § 5/14-1(e). At first blush, section 5/14-2(a)(5) would appear to cover Doe's allegations because she has plausibly alleged the "transfer of signs, signals, writing, images, [and] data"—*i.e.*, a "private electronic communication"—to Deaconess, which was then captured by the website's source code and transmitted to the Third Parties. But this, too, is not the end of the inquiry.

A violation of section 5/14-2(a)(5) presupposes a *completed* interception of a "private electronic communication" because it prohibits the "[u]se[]" of "information"

"obtained from a . . . private electronic communication." Thus, "there must be adequate allegations of a violation of another subsection of section 14-2(a) to invoke section 14-2(a)(5)." *Hannant*, 2025 WL 2413894, at *11. Among the five subsections in section 14-2(a), subsection 14-2(a)(3) is Doe's only option to trigger subsection 14-2(a)(5).[2] Subsection 14-2(a)(3) applies to any person who "[i]ntercepts, records, or transcribes, in a surreptitious manner, any private electronic communication to which he or she is not a party unless he or she does so with the consent of all parties to the private electronic communication."

For Doe, any potential claim under subsection 14-2(a)(3) is met by its requirement that the alleged wrongdoer must be a non-party to the communication in question. Deaconess, however, was a party to these communications. Indeed, the focal point of this entire case is that Doe utilized Deaconess's website and its patient portal to research and manage her care. It is thus apparent that Deaconess was a party to the "private electronic communications" that she claims were improperly intercepted and then transmitted to the Third Parties. And because Deaconess was a party, Doe's claim under 14-2(a)(3) necessarily fails. *See Hannant*, 2025 WL 2413894, at *11 (dismissing IES claim because hospital was party to communications with plaintiff).

For this reason, the Court agrees with Deaconess that Doe has failed to state a claim under the IES. Count VIII of the complaint will be dismissed.

[2] Subsections (a)(1) and (a)(2) apply only to "private conversations." Subsection (a)(4) applies to the production, distribution, and possession of eavesdropping "device[s]." And subsection (a)(5) is triggered only *after* an interception has taken place.

Wiretap Act and Stored Communications Act Claims (Counts IX, X, and XI)

In Counts IX and X, Doe asserts claims under 18 U.S.C. §§ 2511(1) and 2511(3)(a) of the ECPA, also known as the "Wiretap Act." Count XI arises under Title II of the Wiretap Act, 18 U.S.C. § 2701 *et seq.*, commonly referred to as the "Stored Communications Act." The Court begins its discussion with Count IX, which prohibits certain interceptions of electronic communications. It will then address Counts X and XI jointly because they turn on the same legal question.

a. Violation of the Wiretap Act Section 2511(1) (Count IX)

The Wiretap Act provides a private right of action against any person who "intentionally intercepts [or] endeavors to intercept, . . . any wire, oral, or electronic communication," or who intentionally "discloses" or "uses" the contents of an unlawfully intercepted communication. 18 U.S.C. §§ 2511(1)(a), (c) & (d). To make a prima facie case, "[a] plaintiff must show that the defendant (1) intentionally (2) intercepted [or] endeavored to intercept . . . (3) the contents of (4) an electronic communication, (5) using a device." *Stein v. Edward-Elmhurst Health*, 2025 WL 580556, at *3 (N.D. Ill. Feb. 21, 2025) (quoting *In re Google, Inc. Cookie Placement Cons. Priv. Litig.*, 806 F.3d 125, 135 (3d. Cir. 2015)). Under what is known as the "party exception," the Wiretap Act does *not* apply to electronic communication interceptions by "a party to the communication." 18 U.S.C. § 2511(2)(d). The party exception, however, does not apply if the party intercepts the communication "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"—the "crime-tort" exception. *Id.* In short, "one is normally not liable for intercepting her

own communications but may be liable if her conduct satisfies the crime or tort exception." *Hannant*, 2025 WL 2413894, at *3. Here, Doe does not appear to dispute the applicability of the party exception. The question, then, is whether the crime-tort exception applies to retrigger Deaconess's liability under the Wiretap Act.

Deaconess advances three arguments against the application of the crime-tort exception. First, it contends that the crime or tort in question must be "independent" of the communication interception. Second, it argues that the recording must have been made for the specific purpose of harming Doe. And third, it argues, preemptively, that the contents of the intercepted communications did not constitute Individually Identifiable Health Information ("IIHI") under the Health Insurance Portability and Accountability Act ("HIPAA"), so that the alleged disclosure of Doe's information was neither criminal nor tortious. The Court will tackle Deaconess's third argument before turning to the first and second.

Doe contends that the crime-tort exception is triggered here because Deaconess allegedly collected and improperly disclosed her IIHI to the Third Parties in violation of HIPAA. HIPAA defines IIHI as:

> [A]ny information, including demographic information collected from an individual, that—(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) *relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual*, and—(i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

42 U.S.C. § 1320d(6) (emphasis added). HIPAA also generally prohibits anyone from

"knowingly" "disclos[ing] individually identifiable health information to another person." 42 U.S.C. § 1320d-6(a)(3).

Now what exactly "relates" to a person's health? This question is the subject of vigorous advocacy and disagreement in cases like this one. For instance, while a patient's diagnosis of high blood pressure likely "relates" to her health and could qualify as IIHI, what about ancillary information like her participation in a weekly exercise class? As Chief Judge Darrow in the Central District of Illinois aptly put it: "the dividing line is somewhere between precise geolocation data showing that an individual ate in a hospital's cafeteria and such data showing that an individual was in their primary care physician's examination room—the latter could be the basis of a HIPAA violation; the former is probably just lunch." *Hannant*, 2025 WL 2413894, at *4.

Doe has alleged that Deaconess captured specific data points related to her status as a patient at the hospital. Its trackers caught information about her search activities on the website (Compl. ¶ 123), each instance in which she navigated to the website's "Services" page to research medical treatments (*Id.* ¶ 129), specific searches for services, such as the "Emergency Room – Union County Hospital" (*Id.* ¶ 133), and each search for specific providers (*Id.* ¶ 137). She also alleges that her tracked activity on the Deaconess website caused her Facebook feed to serve up advertisements related to the specific "medical conditions and symptoms she searched for and viewed." (*Id.* ¶ 177).

These allegations are far from a sure thing in terms of their ability to fit within HIPAA's definition of IIHI because they do not claim that Deaconess disclosed a condition that *Doe* suffered from. Her search history and even the "conditions" and

"symptoms" she researched are not necessarily related to her; they could concern another person entirely. Nevertheless, on balance, the Court finds that a faithful application of the plausibility standard, with all inferences drawn in Doe's favor, compels a finding that she sufficiently alleged the improper disclosure of her IIHI. It is at least plausible that by capturing Doe's search for specific symptoms, providers, and services, and then disclosing such information to the Third Parties, Deaconess shared information that "related" to her health. Meta also allegedly could and did match the information it received from Deaconess to Doe's Facebook ID. This inference is supported by Doe's allegation that her Facebook feed began showing treatments for the specific conditions she had researched on Deaconess's website. The Court is thus satisfied that Doe has alleged the capture and improper disclosure of IIHI to the Third Parties and can thus invoke the crime-tort exception to sustain her Wiretap Act claim. *See e.g.*, *Kurowski v. Rush Sys. for Health*, No. 22 C 5380, 2023 WL 8544084, at *3 (N.D. Ill. Dec. 11, 2023) (*Kurowski III*) (name, location, and specialty of plaintiff's physician in combination with targeted advertising on Facebook constituted IIHI and supported application of crime-tort exception); *Hartley v. Univ. of Chicago Med. Ctr.*, No. 22 C 5891, 2024 WL 1886909, at *2 (N.D. Ill. Apr. 30, 2024) (same where defendant captured and disclosed plaintiff's search for "specific medical specialists," "various medications," and for "information about sexually transmitted diseases").

Deaconess nevertheless contends that, even if it captured Doe's IIHI, the alleged criminal or tortious activity that would support the crime-tort exception was not "independent" of its "interception" of this information under the Wiretap Act.

To support this argument, Deaconess cites cases from the Second and Third Circuits for the proposition that the crime-tort exception "applies only where the defendant allegedly committed an alleged criminal or tortious act that is independent from the act of recording itself." (Deaconess Mem. in Support of MTD (Doc. 23, p. 17)) (citing *Caro v. Weintraub*, 618 F.3d 94, 99-100 (2d Cir. 2010) and *In re Google*, 806 F.3d at 145 & n.81)). Doe, for her part, claims that *Caro* and *In re Google* are not the law in the "Seventh Circuit." While this is technically true (because *Caro* and *In re Google* are Second and Third Circuit cases respectively), Doe's argument is largely based on a district court case, *Kurowski v. Rush Sys. for Health*, No. 22 C 5380, 2024 WL 3455020, at *4 (N.D. Ill. July 18, 2024) (*Kurowski IV*). She has cited no authority from the United States Court of Appeals for the Seventh Circuit to support her claim that the "Seventh Circuit" has rejected *Caro* and *In re Google*. Still, she insists that this Court "follow the Seventh Circuit" and reject Deaconess's argument. Although the Court is somewhat perplexed by Doe's argument, it is also not persuaded that Deaconess is correct.

In *In re Google*, the plaintiffs attempted to invoke the crime-tort exception based on the defendants' "acquisition" of certain data about them, which they claimed, was tortious under state law. *In re Google*, 806 F.3d at 144-45. The Third Circuit observed, however, that "all authority of which we are aware indicates that the criminal or tortious acts contemplated by § 2511(2)(d) are acts secondary to the acquisition of the communication involving tortious or criminal use of the interception's fruits." *Id.* at 145. The plaintiffs thus could not claim that the unlawful capture of their information by a party to the communication triggered liability under the Wiretap Act because the crime-

tort exception was only triggered by "secondary" acts. *Id.* And for that reason, the court rejected the plaintiffs' interpretation of the crime-tort exception because, under their theory, "the tortious conduct is the wiretapping itself." *Id.*

Similarly, in *Caro*, 618 F.3d at 96, a party to an oral conversation used his phone to record a conversation without informing the other participants. The plaintiff advanced a Wiretap Act claim, arguing that, under the crime-tort exception, the defendant (the person who recorded the conversation) was liable. *Id.* The Second Circuit disagreed. "At the time of the recording the offender must intend to use the recording to commit a criminal or tortious act. Merely intending to record the plaintiff is not enough." *Id.* at 99-100. And because the defendant had no intention of using the recording to commit a crime or tort—*e.g.*, blackmail or stealing business secrets—there was no secondary act that could trigger the exception. *Id.* at 99, 100. The court then concluded that "to survive a motion to dismiss, a plaintiff must plead 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." *Id.* at 100.

Doe's invocation of the crime-tort exception is entirely consistent with *In re Google* and *Caro*. These cases stand for the proposition that the crime or tort that supports the crime-tort exception cannot merge with the "interception" of the communication. There must be a "secondary act" that triggers the exception to reimpose liability on a party to the communication. Here, Doe alleges that Deaconess proceeded in two steps: (i) it captured her PHI and PII by embedding trackers in its website and then (ii) turned around and disclosed that information to the Third Parties. As discussed, the information

that was allegedly intercepted plausibly constituted IIHI. Deaconess's alleged disclosure of it, in turn, plausibly violated HIPAA. The disclosure, not the interception itself, is the secondary act that supports the crime-tort exception.

Finally, Deaconess argues that the crime-tort exception does not apply here because its only goal in collecting and disclosing the information in question was to improve its marketing efforts, which did not "harm" Plaintiff. In support of this argument, Deaconess again cites *Caro* for its observation that the crime-tort exception only applies "if, at the time of the recording, the offender plans to use the recording to harm the other party to the conversation." *Caro*, 618 F.3d at 100. This argument is more simply rejected because, as explained, Doe sufficiently alleged the illegal use of the information–*i.e.*, disclosure to the Third Parties in violation of HIPAA. The fact that Deaconess only sought to use the information for marketing purposes does not remove the case from the purview of the crime-tort exception. "Many crimes and torts are motivated by a desire to make money, and it defies common sense that a clearly harmful act could escape liability as long as it was done for profit." *Kurowski IV*, 2024 WL 3455020, at *5 (internal quotation marks omitted). And even if Deaconess may have had other innocent motives for its capture of Doe's IIHI, its alleged intention to disclose it in violation of HIPAA is enough to trigger the crime-tort exception. *See id.* (holding that "nothing in section 2511(2)(d) requires that a party act with the sole purpose of committing the underlying crime or tort.").

For these reasons, the Court finds that Doe's claim under section 2511(1) of the Wiretap Act (Count IX) survives Deaconess's motion to dismiss.

b. Violation of the Wiretap Act Section 2511(3)(a) (Count X) and Violation of the Stored Communications Act (Count XI)

In Count X, Doe asserts a claim under section 2511(3)(a) of the Wiretap Act, which provides in relevant part that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication." 18 U.S.C. § 2511(3)(a). Count XI advances a related claim under the SCA, which states that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1). Both provisions define an "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15); *see also Id.* § 2711(1) (adopting Wiretap Act definition for SCA). The parties agree that both claims turn on whether Deaconess is a provider of an "electronic communications service."

Deaconess argues that, as a hospital, it is in the business of providing healthcare to its patients, not electronic communications services. Doe, on the other hand, asserts that, in making its website available to the public, Deaconess provided an electronic communications service. She also claims that "the majority of Illinois courts that have addressed ECPA claims in the hospital website privacy context have concluded that ECPA claims have merit in this context." (Doc. 24, p. 23). Deaconess has the better argument here.

First, the Court is, again, confused by Doe's claim that the "majority of Illinois courts" support her position. She cites *Loyola*, 2024 WL 3338941 (N.D. Ill.), *Kurowski IV*,

2024 WL 3455020 (N.D. Ill.), *Hartley*, 2024 WL 1886909 (N.D. Ill.), and *A.D. v. Aspen Dent. Mgmt., Inc.*, No. 24 C 1404, 2024 WL 4119153 (N.D. Ill. Sept. 9, 2024), as authorities that supposedly support the rejection of Deaconess's argument that it is not a provider of an "electronic communications service." But *none* of these cases support this conclusion because none of them addressed the question of whether the defendants were providers of an electronic communications service under the Wiretap Act and the SCA. While it is true that these decisions denied the defendants' motions to dismiss claims under the Wiretap Act, they did so for reasons other than the defendant's role as a provider of an "electronic communications service."

The preponderance of authority, instead, appears to support Deaconess's position that a healthcare provider is not in the business of providing electronic communications services. Indeed, *Kurowski I* found that cases addressing this issue "uniformly hold that companies that merely purchase or use electronic communications services in the conduct of their ordinary business are not themselves electronic communications services." *Kurowski I*, 659 F. Supp. 3d at 940; *see also Garner v. Amazon.com, Inc.*, 603 F. Supp. 3d 985, 1003-04 (W.D. Wash. 2022) ("A company that merely utilizes electronic communications in the conduct of its own business is generally considered a purchaser or user of the communications platform, not the provider of the service to the public."); *St. Johns Vein Ctr., Inc. v. StreamlineMD, LLC*, 347 F. Supp. 3d 1047, 1064 (M.D. Fla. 2018) ("[T]he majority of courts addressing the statute's scope interpret the ECPA to encompass only traditional 'electronic communications services' such as internet service providers, electronic mail providers, telecommunications companies, and remote computing

services") (citation modified). The Central District of Illinois, for its part, has rejected Doe's theory twice. *See Hannant*, 2025 WL 2413894, at *6 (rejecting same argument because "simply operating a website is not enough."); *Doe 1 v. Chestnut Health Sys., Inc.*, No. 1:24-cv-01475, 2025 WL 1616635, at *12 (C.D. Ill. June 6, 2025) (recognizing that "there are many steps involved in an electronic communication that, in their absence, would have prevented the Plaintiffs from communicating with the Defendant's website. That alone does not make each step an electronic communication service.").

The Court finds these authorities persuasive. Deaconess is a hospital. Doe herself alleges that it is in the business of providing "complete inpatient and outpatient care including emergency, medical and surgical services." The fact that it, like most hospitals, operates a website, does not make it a provider of an "electronic communications service" under the Wiretap Act or the SCA. Accordingly, Counts X and XI will be dismissed.

Violation of the Computer Fraud and Abuse Act (Count XII)

In Count XII, Doe advances a claim under the CFAA, 18 U.S.C. § 1030, *et seq*. The CFAA "subjects to criminal liability anyone who 'intentionally accesses a computer without authorization or exceeds authorized access,' and thereby obtains computer information." *Van Buren v. United States*, 593 U.S. 374, 379 (2021) (quoting 18 U.S.C. § 1030(a)(2)). Although initially conceived as a criminal statute, the CFAA now also "provides for a private right of action for anyone that has suffered damage or loss of at least $5,000" due to a violation. *ExactLogix, Inc. v. JobProgress, LLC*, 508 F. Supp. 3d 254, 262 (N.D. Ill 2020); *Dresser-Rand Co. v. Jones*, 957 F. Supp. 2d 610, 613 (E.D. Pa. 2013). Doe proceeds on the theory that Deaconess "exceeded and continues to exceed" its

authorized access to her and the Class's personal computers. (Doc. 1 ¶ 416). To "exceed[] authorized access" under the CFAA means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). Deaconess argues that Doe has failed to state a claim under the CFAA because her allegation that it captured information that she affirmatively sent to it cannot plausibly lead to the conclusion that it "exceeded authorized access" to her computer. Doe responds that she sufficiently alleged a CFAA claim because Deaconess "had *no* authorized access to disclose [her] data." (Doc. 24, p. 24).

The Supreme Court's decision in *Van Buren* tips the scale in favor of Deaconess. There, a police officer used his office's law enforcement database to run a license plate search in exchange for money. *Van Buren*, 593 U.S. at 378. There was no dispute that the officer was authorized access the database—his employer had given him the necessary credentials to do so. *Id.* at 382. The question was whether the CFAA covered his conduct under the "exceeds authorized access" prong of section 1030(a)(2) because he misused his authorized access for an improper purpose. *Id.* The Court examined the phrase "exceeds authorized access" in depth and concluded that a person only "'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him." *Id.* at 396. This is so because "[t]he phrase 'is not entitled so to obtain' [under section 1030(e)(6)] is best read to refer to information that a person is not entitled to obtain by using a computer that he is authorized to access." *Id.*

at 384.

A straightforward application of *Van Buren* compels the rejection of Doe's argument. Her theory that Deaconess violated the CFAA because it "had *no* authorized access to disclose [her] *data*" (second emphasis added) does not explain how it fits into the CFAA's requirement that the wrongdoer "us[e] a computer" in order to "exceed[] authorized access." *Id.* Deaconess was the *recipient* of information that Doe provided. Indeed, the very core of her case is that Deaconess improperly recorded and misused her information after she shared it. Deaconess is thus correct that Doe "does not allege Union County Hospital obtained information from her computer at all, separate and apart from the initial communication—which [Plaintiff] affirmatively instituted." (Deaconess Mem. in Support of MTD (Doc. 23, p. 23)). And similar to *Van Buren*, Deaconess did not obtain any information that was "off limits" to it. That is a fatal defect in Doe's CFAA claim because it invalidates the contention that Deaconess "exceeded authorized access" to her computer. *Cf. CommSolvers LLC v. Wieland North Am., Inc.*, No. 3:21-CV-01234, 2025 WL 786330, at *17 (S.D. Ill. Mar. 12, 2025) (examining "access" requirement under CFAA).

The Court thus concludes that Plaintiff Doe has failed to state a claim under the CFAA. Count XII of her complaint will be dismissed.

CONCLUSION

For these reasons, Deaconess's Motion to Dismiss Doe's Putative Class Action Complaint (Doc. 22) is **GRANTED in part** and **DENIED in part**. Counts III, IV, V, VI, VII, VIII, X, XI, and XII are **DISMISSED without prejudice**.

Doe is **GRANTED** leave to file an amended complaint consistent with this Order on or before **October 29, 2025**.

IT IS SO ORDERED.

DATED: September 29, 2025

NANCY J. ROSENSTENGEL
Chief U.S. District Judge