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

JOEL JUENGER, Individually and on behalf of all others similarly situated, **Plaintiff,** **v.** **DEACONESS HEALTH SYSTEM, INC., DEACONESS ILLINOIS RED BUD REGIONAL HOSPITAL, INC., and RED BUD ILLINOIS HOSPITAL COMPANY, LLC,** **Defendants.**	**Case No. 3:24-CV-2332-NJR**

MEMORANDUM AND ORDER

ROSENSTENGEL, Chief Judge:

In this case, which is nearly identical to another case pending before the undersigned,[1] Plaintiff Joel Juenger alleges that Defendants Deaconess Health System, Inc. and Deaconess Illinois Red Bud Regional Hospital, Inc. ("the Deaconess Defendants") and Red Bud Illinois Hospital Company, LLC ("RBR") (collectively, "Defendants"), violated his privacy rights. Specifically, Juenger claims that RBR used digital analytical tools on its website, which "collected and transmitted patients' Private Information to Facebook and Google, possibly other third parties, without patients' knowledge or authorization." (Doc. 1).

Now before the Court are Defendants' Motions to Dismiss for Failure to State a Claim under Rule 12(b)(6) of the Federal Rules of Civil Procedure. (Docs. 19, 24). As with

[1] *Doe v. Deaconess Illinois Union County Hospital, Inc.*, Case No. 3:24-cv-02284-NJR.

the aforementioned companion case, *Doe v. Deaconess Illinois Union County Hospital, Inc.*, Case No. 3:24-cv-02284-NJR, the Court grants in part and denies in part Defendants' motions to dismiss.

BACKGROUND

The following facts are taken from Juenger's complaint and are accepted as true for the purposes of Defendants' Motions to Dismiss. *Wagner v. Teva Pharms. USA, Inc.*, 804 F.3d 355, 358 (7th Cir. 2016).

RBR, located in Red Bud, Illinois, serves the Southern Illinois region with impatient and outpatient care; emergency, medical and surgical services; rehabilitation; and diagnostic imaging. (Doc. 1 at ¶ 9). It serves as "critical access hospital" with 25 beds and a medical staff of 150. (*Id.* at ¶ 40).

Juenger alleges that RBR's website, https://redbudregional.com/, is equipped with "code-based tracking devices known as "trackers" or "tracking technologies" that collected and transmitted patients' Private Information to Facebook and Google, possibly other third parties, without patients' knowledge or authorization. (*Id.* ¶ 10).

According to Juenger, Defendants encourage patients to use the RBR website, along with their various web-based tools and services (collectively, the "Online Platforms"), to learn about RBR, to find medical providers, to find and research medical services, to access a patient portal, to pay bills, to access medical records, and more. (*Id.* at ¶ 11). He further claims that when he and other putative class members visited RBR's Online Platforms in relation to their past, present, and future healthcare needs and/or to transmit a payment for health care, they thought they were communicating exclusively

with "their trusted healthcare provider." (*Id.* at ¶ 12). Unbeknownst to them, RBR embedded pixels from Facebook and Google, and possibly others, into its Website and Online Platforms, forcing Juenger and the putative class members to transmit intimate details about their medical treatment to third parties without their consent. (*Id.* at ¶ 13).

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 a 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.*). Juenger alleges that "[b]y installing the Meta Pixel on its Website, Defendants effectively planted a bug on Plaintiff's and Class Members' web browsers and compelled them to disclose Private Information and confidential communications to Facebook, without their authorization or knowledge." (*Id.* ¶ 16).

Defendants allegedly "utilized data from these trackers to market their services and bolster their profits." (*Id.* ¶ 20). Facebook, 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.*). Information that RBR's Meta Pixel sent to Facebook included Juenger and the putative

class's browsing activities, including the pages they viewed and the buttons they clicked; information concerning their status as patients such as patient portal activities; information concerning their medical concerns such as the providers they searched for and viewed and the medical services they viewed; and identifying information, such as IP addresses and identifying cookies. (*Id.* at ¶ 21). Juenger alleges this information allows third parties like Facebook to learn of a patient's health conditions, which Facebook then sells to third-party marketers. (*Id.* at ¶ 22). The information could also allow others to infer that a specific patient was being treated for a specific medical condition like cancer, pregnancy, or HIV. (*Id.*).

Defendants allegedly also installed other trackers like Google Analytics, Google Tag Manager, and DoubleClick Ads, which operate similarly to the Meta Pixel and transmit personally identifiable information (PII) and/or personal health information ("PHI") to unauthorized third parties. (*Id.* ¶ 23).

Juenger was a patient at RBR for a head injury beginning in May 2023. (*Id.* at ¶ 87). He used the RBR website multiple times to search for doctors specializing in post-concussion treatment, to pay his medical bills, and to use the patient portal. (*Id.* at ¶ 88). He later began receiving targeted advertisements on Facebook for RBR doctors, related medical services and testing, and vaccinations. (*Id.* at ¶ 92). On information and belief, through its use of the Meta Pixel and other tracking technologies, Juenger claims RBR disclosed to Facebook the pages and content he viewed; his seeking of medical treatment; his status as a patient; his patient portal activity; the medical providers and specialties he searched for; the search results he clicked on; the medical services he viewed; and his

identity via his IP address and/or his Facebook ID. (*Id.* at ¶ 97).

Juenger filed this putative class action in October 2024. (Doc. 1) He advances the following claims on behalf of himself and others whose PHI and PII were allegedly compromised: (i) negligence; (ii) negligence *per se*; (iii) invasion of privacy—intrusion upon seclusion; (iv) breach of implied contract; (v) unjust enrichment; (vi) breach of implied duty of confidentiality; (vii) violation of Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA"); (viii) violation of the Illinois Eavesdropping Statute; (ix) violation of the Electronic Communications Privacy Act ("ECPA" or "Wiretap Act"); (x) violation of the ECPA ("unauthorized divulgence"); (xi) violation of the Stored Communications Act ("SCA"); and (xii) violation of the Computer Fraud and Abuse Act ("CFAA"). (Doc. 1). Defendants filed motions to dismiss the case pursuant to Federal Rule of Civil Procedure 12(b)(6) (Docs. 19, 24), and Juenger filed timely responses in opposition (Docs. 22, 31). RBR also filed a reply brief. (Doc. 32).

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

Defendants have moved to dismiss this action in its entirety, with the Deaconess Defendants adopting and relying on the briefing in *Doe*. Both Defendants also separately address the Illinois claims raised here—implied duty of confidentiality and the ICFA—that were not raised in *Doe*.

I. Negligence, Negligence *Per Se*, and Breach of Implied Contract (Counts I, II, IV)

Defendants first argue that Juenger's negligence and breach of contract claims must fail because he has not alleged facts demonstrating that he suffered actual damages. While Juenger broadly alleges damages including (1) loss or invasion of privacy, (2) economic or contract-based damages, (3) mitigation measures, and (4) emotional distress, Defendants assert that none of these are sufficient to support his negligence or breach of contract claims. (*Id.*). RBR also argues that the disclosed information is not PHI in the first place.

1. Personal Health Information (PHI)

In arguing that Juenger has not alleged the disclosure of PHI, RBR notes that Juenger relies on guidance issued by the Office for Civil Rights at the U.S. Department of Health and Human Services, which stated that when an advertising technology connects (1) an individual's IP address with (2) a visit to a public webpage that addresses specific health conditions or healthcare providers, this combination—known as the "Proscribed Combination"—constitutes PHI under HIPAA. (Doc. 1 at ¶ 124). But in *American Hospital Association v. Becerra*, RBR argues, a federal district court found that without knowing a website visitor's "subjective motive," the resulting metadata cannot be considered individually identifiable information. 2024 WL 3075865, at *7 (N.D. Tex. June 20, 2024) ("The mere fact that an online tracking technology connects the IP address of a user's device (or other identifying information) with a visit to a webpage addressing specific health conditions or listing health care providers is not sufficient . . . to constitute IIHI [individually identifiable health information]."). Because Juenger has failed, as a matter of law, to allege that RBR disclosed any PHI, RBR argues he has failed to assert any actionable privacy interest that could give rise to damages.

In response, Juenger avers that RBR has oversimplified his allegations. Juenger alleged Defendants disclosed the pages and content he viewed, his seeking of medical treatment, his status as a patient, information regarding his patient portal activity, the specialties of the medical providers he searched for and viewed, the names of the medical providers he searched for and viewed, the search results he clicked on, the medical services he viewed, and his identity via his IP address and/or "c_user" cookie and/or

FacebookID. These are all sufficient to constitute PHI or PII, and RBR has failed to explain how they are not. Juenger also argues that *Becerra*, which is not binding on this Court, was decided on summary judgment and presented a very limited question: whether HHS exceeded its rule-making authority. The answer to that question does not affect whether a contract was breached under Illinois law, whether a tort was committed under Illinois law, whether any Illinois statutes were violated, or whether standards of care informed by HIPAA or the FTC Act were violated. Indeed, Juenger argues, none of his claims turn on interpreting the HHS Guidance.

The Court agrees with Juenger that, for the purposes of Defendants' motions to dismiss, he has sufficiently alleged that Defendants disclosed his PHI or PII to third parties.

2. *Actual Damages*

In Illinois, a negligence claim can be based on the loss of privacy. *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). Here, Juenger alleges that he and the putative class suffered "decreased value of [their] private information, emotional harm, loss of privacy, the revenues, profits, and savings attributable to Defendant's unauthorized sale of [their] Private Information, and increased risk of future harm" (Doc. 1 at ¶ 99), as well as "embarrassment, humiliation,

frustration, and emotional distress." (*Id.* at ¶ 230). These damages are also cognizable in a negligence action. *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 Juenger has pled cognizable damages with respect to Counts I and II.[2]

The same cannot be said for Juenger's implied breach of contract claim. "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*

[2] 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 Juenger links his negligence *per se* claim to violations of the Health Insurance Portability and Accountability Act ("HIPAA") and its associated regulations, he has not identified HIPPA, 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 Defendants' motions to dismiss at this stage because they have 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.").

v. Christie Bus. Hold. Co., 230 N.E.3d 162, 169 (Ill. App. Ct. 2023).

Juenger has failed to sufficiently allege actual damages, as emotional damages, the risk of future harm, and the loss of privacy 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 Juenger'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 Court of Appeals has questioned whether a person even holds a property right in his personal information. *See id.* ("This court is unaware of any case law holding that a person has a property right in her personal information."). 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 Defendants' alleged disclosure of Juenger's personal information are insufficient because Juenger had a contract with Defendants to receive medical care. (Doc. 1 at ¶ 259). He did not enter into a profit-sharing agreement whereby Defendants would market and sell his personal information. To accept lost revenues and profits as cognizable damages in support of his implied 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. 3d 836, 845-46 (N.D. Ill. 2023) (*Kurowski II*) (similar damages did not satisfy "actual damages" requirement); *see also Mount v. PulsePoint, Inc.*, 2016 WL 5080131, at *6, 13 (S.D.N.Y. Aug. 17, 2016), *aff'd* 684 F. App'x 32, 36 (2nd Cir. 2017) ("plaintiffs do not allege that

PulsePoint's data collection practices actually deprived them of any opportunity to sell their own personalized information"); *Williams v. TMC Health*, 2024 WL 4364150, at *9 (D. Ariz. Sept. 30, 2024) ("the complaint is devoid of allegations indicating Plaintiffs ever intended to profit from their data or even had some other avenue for profiting from their data").

For these reasons, the Court finds that Juenger has failed to allege actual damages that can support his breach of implied contract claim. Count IV will be dismissed.

II. Invasion of Privacy – Intrusion upon Seclusion (Count III)

Juenger's invasion of privacy—intrusion upon seclusion claim is based on his allegations that he and the putative class had a reasonable expectation of privacy in their communications with Defendants via the RBR website, that they communicated sensitive PHI and PII intended only for Defendants to receive, that they understood Defendants would keep this PHI and PII private, and that Defendants disclosed this information to Facebook and other third parties, without their authorization or knowledge. (Doc. 1 at ¶¶ 247-49). Furthermore, Defendants' disclosure of this information was an intentional intrusion on their solitude or seclusion in their private affairs. (*Id.* at ¶ 250).

RBR argues that this invasion of privacy claim fails because the alleged harm flows from the subsequent *disclosure* of the information, not from an initial *intrusion*. Citing the Seventh Circuit's holding in *Thomas v. Pearl*, 998 F.2d 447, 452 (7th Cir. 1993), they argue that a claim for invaded seclusion is not viable in Illinois "if the harm flows from the publication rather than the intrusion" itself. Defendants point to other cases from the Northern District of Illinois, which applied this holding more recently in similar

situations. *See Kurowski II*, 683 F.Supp.3d at 848-49 ("The harm caused by Rush, if any, continues to be its alleged disclosure of the Kurowski's private health information."); *Hartley v. University of Chicago Medical Center*, 2023 WL 7386060, at *2-3 (N.D. Ill. Nov. 8, 2023) ("*Hartley II*") ("Since Plaintiff is complaining about what she thinks UCMC told Facebook, her complaints are with the publication, and not any intrusion").

The Northern District of Illinois addressed a nearly identical invasion of privacy claim based on intrusion upon seclusion in *Kurowski*. 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. *Kurowski II*, 683 F.Supp.3d at 848-49. In addressing the plaintiff's invasion of privacy claim, the court 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*. These allegations, the court 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 . . . ." *Id.* at 848-49 (quoting *Dinerstein*, 484 F. Supp. 3d at 594 (quotation marks omitted)). Thus, "disclosures of private personal information do not support a claim for unauthorized intrusion." *Dinerstein*, 484 F. Supp. 3d at 594.

The Court finds *Kurowski II*'s reasoning, and the authorities it relied on, persuasive. Juenger's allegations here are nearly identical to those offered in *Kurowski II*. He claims that Defendants improperly captured and disclosed his PHI and PII as he used its website and patient portal. Nowhere has he alleged that Defendants 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, Defendants were the *intended recipient*s of the information in question.

For these reasons, Juenger's invasion of privacy claim based on intrusion upon seclusion (Count III) will be dismissed.

III. Unjust Enrichment (Count V)

As in *Doe*, the Court makes "short work" of Juenger'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.

Juenger alleges that he was injured by Defendants' improper capture and disclosure of his PHI and PII. His unjust enrichment claim and other statutory and common law claims assign liability based on this conduct. Therefore, the unjust

enrichment claim "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, Juenger 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, the unjust enrichment claim in Count V will be dismissed.

IV. Breach of Implied Duty of Confidentiality (Count VI)

In Count VI, Juenger alleges a breach of the implied duty of confidentiality under Illinois law. Specifically, he claims there is a duty of confidentiality implied in every healthcare provider and patient relationship, akin to an implied contract, such that healthcare services providers may not disclose confidential information acquired through the healthcare provider-patient relationship. (Doc. 1 at ¶ 280). Here, he claims Defendants agreed to keep his and the putative class members' PHI and PII confidential as part of establishing and maintaining healthcare services in the provider/patient relationship between Defendants and Plaintiffs. (*Id.* at ¶ 279).

"Illinois courts have not recognized a cause of action for breach of confidentiality for the unauthorized disclosure of a patient's medical information," and federal courts have declined plaintiffs' "invitation[s] to recognize one." *Kurowski II*, 683 F. Supp. 3d at

845 (citing *Dinerstein*, 484 F. Supp. 3d at 594-95). In *Dinerstein*, the court explained that the Seventh Circuit "consistently ha[s] held that it is not [district courts'] role to break new ground in state law. *Id.* The *Kurowski* court followed suit, stating: "As far as the Court is aware, a common law cause of action for breach of confidentiality remains unavailable in Illinois, and Kurowski has not offered any justification for the Court to 'break new ground' here by recognizing one." *Id.*

Likewise, this Court declines to recognize a claim for breach of the implied duty of confidentiality under Illinois law. Count VI will be dismissed.

V. ICFA (Count VII)

Count VII of Juenger's Complaint alleges Defendants violated the ICFA. "In order to state a claim under the ICFA, a plaintiff must show: (1) a deceptive or unfair act or promise by the defendant; (2) the defendant's intent that the plaintiff rely on the deceptive or unfair practice; and (3) that the unfair or deceptive practice occurred during a course of conduct involving trade or commerce." *Camasta v. Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 739 (7th Cir. 2014) (internal quotation marks omitted). Moreover, an individual suing under the ICFA must "plead that the deceptive or unfair act caused her to suffer actual damages, meaning pecuniary loss." *Benson v. Fannie May Confections Brands, Inc.*, 944 F.3d 639, 647 (7th Cir. 2019).

Here, Juenger asserts Defendants used unfair and deceptive acts or practices in the conduct of trade or commerce when they encouraged him to use their website while representing their commitment to privacy, promised they would not use his and the class members' PHI for undisclosed purposes without their permission, disclosed the PHI

anyway, and Juenger and the class members relied on Defendants' representations in using the website and believing they were communicating only with their trusted healthcare provider. (Doc. 1 at ¶ 294). Juenger further alleges that, as a result of Defendants' unfair and deceptive acts and practices, he and the putative class suffered damages in that: sensitive and confidential information that "Plaintiff and Class Members intended to remain private is no longer private; Defendants eroded the essential confidential nature of the doctor-patient relationship; Defendants took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value; Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendants' duty to maintain confidentiality; and Defendants' actions diminished the value of Plaintiff's and Class Members' personal information." (*Id.* at ¶ 306).

None of these theories, which relate to Juenger's privacy rights, state a claim for actual damages under the ICFA. *See Khorloo v. John C. Heath Attorney at Law*, No. 18 C 1778, 2020 WL 1530735, at *2 (N.D. Ill. Mar. 31, 2020) ("[T]he Court could not locate any Illinois case law suggesting that privacy violations . . . provide a basis for actual damages under the ICFA. It seems unlikely that the statute allows plaintiffs to recover damages for privacy violations because the ICFA is concerned with fraudulent or unfair advertising, not with individual privacy rights."). Thus, Juenger's ICFA claim fails.

VI. Violation of the Illinois Eavesdropping Statute (Count VIII)

In Count VIII, Juenger asserts a claim under the Illinois Eavesdropping Statute,

720 ILCS 5/14, *et seq.* ("IES"). The IES 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).

RBR argues that Juenger cannot rely on section 14-2(a)(2) to assert an IES claim because it applies only to "private conversations," and the "private electronic communications" at issue were *with the Defendants*. (Doc. 2 at ¶ 318). But in doing so, RBR cites only to 720 ILCS 5/14-2(a)(3), which provides that a person commits eavesdropping when he or she knowingly and intentionally "[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."

But Section 14-2(a)(2), on which Juenger relies, states that it is a violation of the statute to: "use[] 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)(emphasis added). Juenger also alleges that an eavesdropping device means "any device capable of being used to hear or record oral conversation or intercept, or transcribe electronic communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means." 720 ILCS 5/14-1(a). And the eavesdropping devices used here include:

"Plaintiff's and Class Members' personal computing devices; Plaintiff's and Class Members' web browsers; Plaintiff's and Class Members' browser-managed files; Facebook's Pixel; internet cookies; other tracking technology including Google Analytics with Google Tag Manager ("GTM"), and DoubleClick Ads; Defendants' computer servers; third-party source code utilized by Defendants; and computer servers of third-parties (including Facebook) to which Plaintiff's and Class Members' communications were disclosed." (Doc. 1 at ¶ 326).

Because Juenger has alleged that Defendants used an eavesdropping device for the purpose of transmitting all or part of a private conversation to which Defendants were a party, without the consent of all other parties to the conversation, he has properly asserted a claim under the Illinois Eavesdropping Act.

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

In Counts IX and X, Juenger 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.

1. *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.

RBR argues that Juenger cannot state a claim under § 2511 because the crime-tort exception does not apply. RBR asserts that, "[i]n order for an act to be done with a 'criminal or tortious purpose,' the offender must 'plan[] to use the recording to harm the other party to the conversation[.]'" *Caro v. Weintraub*, 618 F.3d 94, 99-100 (2d Cir. 2010). Here, however, there are no allegations that RBR "intercepted" Juenger's web browsing activity with the "primary motivation or purpose" of committing a separate tort against him. Although Juenger makes boilerplate allegations to this effect, RBR contends, he alleges zero facts to make it plausible that RBR possessed a tortious or criminal purpose.

(Doc. 1 at ¶ 351) ("In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of its Website, Defendants' purpose was tortious, criminal and designed to violate federal and state legal provisions . . . .").

Junger contends that the crime-tort exception is triggered because Defendants violated HIPAA, and a disclosure that violates HIPAA is a violation of law that is independent of a violation of the ECPA. Indeed, Juenger alleges that Defendants proceeded in two steps: (i) they captured his PHI and PII by embedding trackers in its website and then (ii) disclosed that information to the Third Parties. The disclosure, not the interception itself, is the secondary act that supports the crime-tort exception.[3]

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

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

In Count X, Juenger 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

[3] For a more thorough discussion of the crime-tort exception, *see Doe v. Deaconess Illinois Union County Hospital, Inc.*, No. 3:24-CV-02284-NJR, 2025 WL 2771415, **8-10 (S.D. Ill. Sept. 29, 2025).

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 RBR is a provider of an "electronic communications service."

RBR argues that it is a hospital, while an electronic communication service provider is the provider of the underlying service which transports the data, such as an internet service provider or a telephone company. Juenger asserts that, by making its website available to the public, RBR provided an electronic communications service. He also contends that Illinois federal courts concluded that ECPA claims "have merit in this context." (Doc. 24, p. 23).

None of the Illinois cases cited by Juenger, however, 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 Defendants' 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 Juenger'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. RBR is a hospital. 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.

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

Finally, in Count XII, Juenger 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).

Here, Juenger alleges that Defendants "exceeded and continue to exceed" their authorized access to his and the class's personal computers. (Doc. 1 at ¶ 384). 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). Juenger further claims that the secret transmission of his PHI and PII, which were never intended for public consumption, caused a loss of at least $5,000, and that Defendants' conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally identifiable data and content of Juenger's PHI and PII being made available to Defendants, Facebook, Google, and/or other third parties without adequate legal privacy protections.

RBR argues that these allegations are insufficient to state a claim under the CFAA because the Supreme Court has held, based on CFAA's statutory language, that "damage" and "loss" under the CFAA are limited to "technological harms" affecting computer systems and data such as the corruption of files. *See Van Buren v. United States*, 593 U.S. 374, 376, 391-92 (2021). Moreover, the disclosure of website browsing history to third-party advertisers does not threaten the *health or safety of the public*. Finally, under

Van Buren, a person only "exceeds authorized access" when they have permission to access a computer but then obtains information located in an area of a computer they are not authorized to access. *Id.* at 396. Juenger makes no such allegations here.

The Supreme Court's decision in *Van Buren* is dispositive. 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 Juenger's argument. His theory that Defendants violated the CFAA because they "had *no* authorized access to disclose their data" 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.* Defendants were the *recipients* of information that Juenger provided. As argued by RBR, there are no allegations in the Complaint that this browser-server

interaction amounts to the acquisition of "information located in particular areas of the computer—such as files, folders, or databases—that are off limits to [RBR]." *Van Buren*, 593 U.S. at 396. And similar to *Van Buren*, Defendants did not obtain any information that was "off limits" to them. The Court thus concludes that Juenger has failed to state a claim under the CFAA. Count XII of the complaint will be dismissed.

CONCLUSION

For these reasons, Defendants' Motions to Dismiss for Failure to State a Claim (Docs. 19, 24) are **GRANTED in part** and **DENIED in part**. Counts III, IV, V, VI, VII, X, XI, and XII are **DISMISSED without prejudice**. Juenger shall proceed on Counts I, II, VIII and IX.

IT IS SO ORDERED.

DATED: September 30, 2025

NANCY J. ROSENSTENGEL
Chief U.S. District Judge