

the plaintiff's complaint and draws all reasonable inferences from those facts in the plaintiff's favor. *Kubiak v. City of Chicago*, 810 F.3d 476, 480-81 (7th Cir. 2016).

According to the complaint, Duly is a healthcare provider. Doc. 34 ¶ 44. It operates a website, patient portal, and application used by patients to book and manage appointments, communicate symptoms and other health-related information to their doctors, and search for medical conditions and treatment options. *Id.* ¶¶ 7-8. The parties describe the website, portal, and application as "web properties." *Id.* ¶ 9.

The complaint alleges that Duly uses two pieces of software to track how its users interact with its web properties. The first is the Meta Tracking Pixel ("Pixel"), which records information about how a person uses Duly's web properties and transmits that information to Meta. Doc. 34 ¶¶ 11, 17. The type of information Pixel tracks includes pages visited, buttons clicked, and text entered into online searches and forms. *Id.* ¶ 13. The second tool is Facebook's Conversions Application Programming Interface ("CAPI"), which captures "submissions, keystroke events, and other user actions performed by the user" for subsequent transmission to Meta. *Id.* ¶¶ 74-75. User information captured by Pixel or CAPI is used by Meta to target those individuals with advertisements tailored to information they have shared with Duly. *See, e.g., id.* ¶¶ 12, 21-22.

Plaintiffs allege that they used and accessed Duly's website and portal to find providers, seek treatments, and make appointments. Doc. 34 ¶ 57. In so doing, Plaintiffs communicated personally identifiable health information to Duly, which was captured by Pixel and CAPI and then transmitted to Meta. *Id.* ¶¶ 59, 72, 83, 89-93. Meta then used this information to target Plaintiffs with spam and advertisements based on the information received from Duly. *See id.*

¶¶ 249-50, 267-68, 285-86. According to the complaint, all of this was done without Plaintiffs' knowledge, authorization, or consent. *Id.* ¶ 94.

Plaintiffs brought eight claims against Duly in their complaint. Five of those claims have now been withdrawn in response to Duly's motion to dismiss. The three remaining claims allege violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2511(1)(a), the Illinois Eavesdropping Statute, 720 ILCS 5/14-2(a)(2), (a)(5), and common law negligence.

I. ECPA Claim

The Electronic Communications Privacy Act ("ECPA"), also known as the Wiretap Act, provides that any person who "intentionally intercepts ... any wire, oral or electronic communication" may be subject to criminal liability as well as civil suit. 18 U.S.C. § 2511(1)(a), (5)(a)(ii), 18 U.S.C. § 2520. The Wiretap Act provides an exception for liability, known as the "party exception" or one-party consent rule, whereby

[i]t shall not be unlawful ... to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception *unless such communication is intercepted for the purpose of committing any criminal or tortious act*

18 U.S.C. § 2511(2)(d) (emphasis added). In other words, ECPA liability does not extend to individuals who record their own conversations, even if the other participants in that conversation did not authorize the recording, so long as the recording is not made for the purpose of committing some other crime or tort. In the ECPA context, "when the law speaks of recording conversations with a criminal or tortious purpose, it has ... regard for the intended use of the recordings." *In re High Fructose Corn Syrup Antitrust Litig.*, 216 F.3d 621, 626 (7th Cir. 2000).

The parties do not dispute that Duly was party to Plaintiffs' intercepted communications. Instead, the parties focus their briefing on whether the ECPA's "purpose of committing any criminal or tortious act" carve-out applies to the facts of this case. Plaintiffs argue it does

because Duly violated the Health Insurance Portability and Accountability Act (“HIPAA”) when it transmitted details of their web usage to Meta. In relevant part, HIPAA imposes criminal penalties for knowingly disclosing individually identifiable health information to a third party, 42 U.S.C. § 1320d-6, where such information is defined as

any information, including demographic information collected from an individual, that—
(A) is created or received by a health care provider ... (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).

Duly’s primary argument is that the ECPA’s crime-tort carve-out does not apply because Duly’s purpose in transmitting Plaintiffs’ health information to Meta was to conduct lawful digital marketing. Duly also argues that Plaintiffs have not plausibly alleged any tortious or criminal purpose by Duly to put the carve-out into play.

Duly’s argument arises largely from its interpretation of *Desnick v. American Broadcasting Companies, Inc.*, 44 F.3d 1345 (7th Cir. 1995). In *Desnick*, a television network sent persons equipped with concealed cameras to ophthalmology clinics to pose as patients and covertly record their conversations with clinic staff. *Id.* at 1348. The network later used clips from these recordings in an exposé that suggested the clinics had engaged in Medicare fraud by recommending unnecessary cataracts surgeries to elderly patients. *Id.* This prompted the ophthalmology clinics to sue the network for defamation (for the exposé) and for violating the ECPA (for the covert recording), among other claims. *Id.* at 1349. On appeal from a motion to dismiss, the Seventh Circuit considered whether the ECPA’s crime-tort carve-out barred the television network from invoking the one-party consent exception, given the allegedly defamatory use to which the recordings ultimately were put. It concluded the crime-tort carve-

out did not apply because there was “no suggestion that the defendants sent the testers into the [clinic’s] offices for the purpose of defaming the plaintiffs.” *Id.* at 1353. Rather, the testers’ “purpose, by the plaintiffs’ own account, was to see whether the [clinic’s] physicians would recommend cataract surgery on the testers.” *Id.*

The Court does not read *Desnick* to hold that the crime-tort carve-out never applies if there was some lawful purpose for intercepting a communication. When statutes speak in terms of an illicit “purpose,” the fact that there may also have been some legitimate reason motivating the defendant’s conduct does “not sanitize the illegitimate one.” *Securities & Exchange Com’n v. Lipson*, 278 F.3d 656, 661 (7th Cir. 2002) (interpreting insider trading statute), citing *Sussman v. Am. Broadcasting Companies, Inc.*, 186 F.3d 1200, 1202 (9th Cir. 1999) (interpreting the crime-tort carve-out to the ECPA’s one-party exception and concluding that “the existence of a lawful purpose does not mean that the interception is not also for a tortious or unlawful purpose”); *see also Village of Arlington Heights v. Metropolitan Housing Development Corp.*, 429 U.S. 252 (1977) (interpreting Equal Protection Clause and stating that a plaintiff does not need “to prove that the challenged action rested solely on racially discriminatory purposes” so long as discriminatory purpose was a “motivating factor”); *U.S. v. McGuire*, 627 F.3d 622, 624-26 (7th Cir. 2010) (interpreting statute that criminalizes travel for the purpose of having sex with a minor to include travel that also had a legitimate purpose). In *Desnick* the problem was not that the defendants’ conduct had dual purposes, but that the illicit purpose did not exist at all at the time of the defendants’ interceptions. *Desnick* stands for the proposition that the crime-tort carve-out “requires a court to look to the party’s intentions at the time it committed the alleged Wiretap Act violation” and that the carve-out will not apply just because a “party later misused an intercepted communication in furtherance of a separate crime” or tort. *Kurowski v. Rush Sys. for*

Health, 2024 WL 3455020, at *4 (N.D. Ill. July 18, 2024); *see also Caro v. Weintraub*, 618 F.3d 94, 99-100 (2d Cir. 2010) (considering *Desnick* and interpreting the crime-tort carve-out to apply only if “[a]t the time of the recording the offender ... intend[s] to use the recording to commit a criminal or tortious act” independent of the act of recording). This is not a surprising conclusion: requiring *mens rea* to be present at the time the offense is committed is a basic and foundational principle of criminal law. *See, e.g., Quarles v. U.S.*, 587 U.S. 645, 651 (2019) (discussing the necessity of the *mens rea* occurring contemporaneously with the *actus reus* in the context of a burglary prosecution).

The Court is unpersuaded by Duly’s citations to out-of-Circuit opinions. *See* Doc. 40 at 13-14, citing *In re Google Inc. Gmail Litig.*, 2014 WL 1102660, at *18 n. 13 (N.D. Cal. Mar. 18, 2014); *Rodriguez v Google LLC*, 2021 WL 2026726, at *6 n. 8 (N.D. Cal. May 21, 2021); *Katz-Lacabe v. Oracle Am., Inc.*, 668 F.Supp.3d 928, 945 (N.D. Cal. 2023); *In re DoubleClick Inc. Privacy Litig.*, 154 F.Supp.2d 497, 515-19 (S.D.N.Y. 2001). According to Duly, these decisions establish that ECPA’s crime-tort carve-out does not apply to recordings made for a commercial or financial purpose. Each of Duly’s citations relies upon *DoubleClick*, a case where the court declined to apply the crime-tort carve-out because plaintiffs failed to allege that the offender’s “‘primary motivation’ or a ‘determining factor’ in its actions [was] to injure plaintiffs tortiously.” *In re DoubleClick*, 154 F.Supp.2d at 518.¹ The *DoubleClick* court then commented that “everything in the amended Complaint” indicated that the offender’s conscious purpose was “pursuit of commercial gain—a goal courts have found permissible under § 2511(2)(d).” *Id.* It seems to the Court that the outcome in *DoubleClick* was driven largely by plaintiffs’ failure

¹ The “primary motivation” or “determining factor” legal standard derives from *U.S. v. Dale*, which held that to invoke the crime-tort exception, all that must be shown is that “some determinative factor in the [interception] was impermissible.” 991 F.2d 819, 842 (D.C. Cir. 1993) (emphasis added).

allege a criminal or tortious purpose, which—as the Court will explain below—is not the situation here.²

Guided by these principles, the Court turns to whether Plaintiffs have adequately alleged a criminal or tortious purpose at the time their communications were intercepted. Plaintiffs have alleged that Meta’s Pixel and CAPI tools are designed to record and transmit information to Meta, and that Duly made the affirmative choice to use these tracking tools in order to “surreptitiously share its patients’ private and protected communications ... including communications that contain ... private information.” Doc. 34 ¶¶ 56, 72. Each of the Plaintiffs have also alleged facts supporting the inference that Duly did in fact disclose their individually identifiable health information to Meta. Plaintiff Mayer alleges that after conducting searches and submitting information to Duly’s web properties regarding her specific medical condition, she began to receive spam and advertisements on her Facebook and other social media accounts related to that medical condition. *Id.* ¶¶ 249-50. Plaintiffs Massarelli and Murphy allege similar experiences of submitting condition-specific information to Duly web properties and, afterwards, receiving advertisements on Facebook and social media about those conditions. *Id.* ¶¶ 267-68, 285-86. Although the evidence adduced during discovery could show otherwise, based on the facts as currently alleged, Duly shared confidential health information with Meta purposefully. That Duly may have intended to make money from sharing this information—either through benefits from Meta or increased business for Duly due to better-targeted advertisements—is immaterial (at least at this stage of proceedings). Protected health information has monetary

² The Court also does not find persuasive Duly’s reliance on *Cohen v. Casper Sleep Inc.*, 2018 WL 3392877, at *3-4 (S.D.N.Y. July 12, 2018), which the Court believes is consistent with *Desnick* insofar as the *Cohen* court analyzed whether the offender’s “primary motivation *at the time of the* alleged interception was to commit a tort,” and concluded that the plaintiffs there failed to allege any such motivation.

value; it is no defense to a HIPAA charge that one violated HIPAA only because they wanted to make money by doing so. Duly does not dispute that it is a healthcare provider or that providing condition-specific information to Meta “discloses individually identifiable health information to another person.” 42 U.S.C. § 1320d-6(a)(3). Thus, the Court concludes Plaintiffs have plausibly alleged that Duly intended to send their individually identifying health information to third-party Meta, in violation of HIPAA. Joining with other courts that reached the same conclusion on similar facts, the Court finds that Plaintiffs’ allegations are sufficient to invoke the crime-tort carve-out to the ECPA’s one-party consent exception. *Stein v. Edward-Elmhurst Health*, 2025 WL 580556, at *4-5 (N.D. Ill. Feb. 21, 2025) (collecting cases); *Kurowski v. Rush Sys. for Health*, 2023 WL 8544084, at *3 (N.D. Ill. Dec. 11, 2023). Accordingly, the Court denies Duly’s motion to dismiss Plaintiffs’ ECPA claim.

II. Illinois Eavesdropping Statute Claim

Plaintiffs’ next claim is brought under Sections 14-2(a)(2) and (a)(5) of the Illinois Eavesdropping Statute.

Section 14-2(a)(2) prohibits a person from using “an eavesdropping device, in a surreptitious manner, for the purpose of overhearing, 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 of the parties to the private conversation.” 720 ILCS 5/14-2(a)(2). The statute defines “private conversation” as an “oral communication between 2 or more persons, whether in person or transmitted between the parties by wire or other means.” 720 ILCS 5/14-1(d). Duly argues that Plaintiffs’ 14-2(a)(2) claim must fail because Plaintiffs did not allege that any oral communications were intercepted. Plaintiffs respond that a 2014 legislative amendment to the Eavesdropping Statute expanded the definition of “private conversation” to reach non-oral

communications. Specifically, Plaintiffs rely on a 2014 legislative amendment to the statute's definition of "private conversation," wherein the modifier "whether in person or transmitted between the parties by wire or other means" was added to the phrase "oral communication between 2 or more persons." *See* Doc. 44 at 19. The problem with this reading is that it is not supported by the statute's text, as the amendment did not remove the word "oral" from the definition. Rather, the amendment made it clear that the statute is intended to reach oral conversations in all forms, whether via phone, Zoom, or any other technology. Because Plaintiffs complain about typed communications and not oral ones, they have not alleged a Section 14-2(a)(2) violation.

Nor have Plaintiffs alleged a Section 14-2(a)(5) violation. Section 14-2(a)(5) of the Eavesdropping Statute bars a person from using or disclosing "any information which he or she knows or reasonably should know was obtained from a private conversation or private electronic communication *in violation of this Article*, unless he or she does so with the consent of all of the parties." 720 ILCS 5/14-2(a)(5) (emphasis added). Section 14-2(a)(5) operates as a mechanism to punish not just those who improperly record communications, but also those who use or disclose the improper recordings. But the basic premise remains that the recordings must be improper (or, to use the precise words of the statute, "obtained ... in violation of this Article"). Therefore, Plaintiffs must first allege a violation of Section 14-2(a)(1), (a)(2), (a)(3), or (a)(4) to plead a claim under Section 14-2(a)(5).

Section 14-2(a)(1) and (a)(2) proscribe transmission and recording of private conversations. As the Court has explained, "private conversations" is defined to include only oral communications, which Plaintiffs have not alleged. Nor do Plaintiffs allege any violation of Section 14-2(a)(4), which extends liability to manufacturers and distributors of eavesdropping

devices. 720 ILCS 5/14-2(a)(4). That leaves Section 14-2(a)(3), which prohibits surreptitious interception and recording of “any private electronic communication [to] which [the eavesdropper] is not a party unless he or she does so with the consent of all parties to the private electronic communication.” 720 ILCS 5/14-2(a)(3). Duly argues that Plaintiffs have not alleged any Section 14-2(a)(3) violation because Duly is a party to the at-issue communications. The Court agrees. Section 14-2(a)(3) specifically states that it reaches only electronic communications to which the eavesdropper “is not a party.” To interpret Section 14-2(a)(3) as also reaching communications where the eavesdropper is a party would render that text a nullity, which the Court will not do. *See Williams v. Taylor*, 529 U.S. 362, 404 (2000) (“It is ... a cardinal principle of statutory construction that [courts] give effect, if possible, to every clause and word of a statute”) (internal quotation omitted). Because Duly was party to the communications alleged to have been sent impermissibly to Meta, Plaintiffs have not pled a Section 14-2(a)(3) violation as is required to allege a Section 14-2(a)(5) claim. Accordingly, Plaintiffs’ claims under the Eavesdropping Statute are dismissed.

III. Negligence Claim

Finally, Plaintiffs bring a negligence claim against Duly under Illinois common law. “To plead a cause of action for negligence a plaintiff must plead that the defendant owed a duty of care to the plaintiff, that the defendant breached that duty, and that the breach was the proximate cause of the plaintiff’s injuries.” *Cowper v. Nyberg*, 28 N.E.3d 768, 772 (Ill. 2015) (internal citation omitted). Duly argues that Plaintiffs have not sufficiently pled a duty of care cognizable under Illinois law.

“Whether a duty is owed presents a question of law.” *Swearingen v. Momentive Specialty Chemicals, Inc.*, 662 F.3d 969, 972 (7th Cir. 2011). “The concept of duty in negligence cases is

involved, complex, and nebulous.” *Simpkins v. CSX Transp., Inc.*, 965 N.E.2d 1092, 1096 (Ill. 2012). Illinois courts have “long recognized that ‘every person owes a duty of ordinary care to all others to guard against injuries which naturally flow as a reasonably probable and foreseeable consequence of an act, and such a duty does not depend upon contract, privity of interest or the proximity of relationship, but extends to remote and unknown persons.’” *Id.* at 1097 (internal citation omitted). Thus, whether a relationship “sufficient to establish a duty of care” exists depends largely on “considerations of policy” that apply to a case’s specific circumstances. *Id.*

“A tort duty can derive from the common law or from statute.” *People ex rel. Dept. of Labor v. Valdivia*, 955 N.E.2d 631, 635 (Ill. App. Ct. 2011). A statute may create a duty “expressly, or it may do so impliedly where it is designed to protect human life or property.” *Rommel v. Illinois State Toll Highway Authority*, 938 N.E.2d 1163, 1168 (Ill. App. Ct. 2010). And some statutes impose duties on specific classes of persons that, if breached, may give rise to negligence claims against them. *See Cowper*, 28 N.E.3d at 773 (describing statutes that imposed duties on court clerks which could support a negligence action).

In this case, the Court concludes that Illinois law imposes a duty on collectors of personal information to undertake reasonable measures to keep that information safe. For example, the Illinois Personal Information Protection Act (“PIPA”) requires that data collectors “implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.” *Flores v. Aon Corp.*, 242 N.E.3d 340, 353 (Ill. App. Ct. 2023), citing Pub. Act. 99-503 (eff. Jan. 1, 2017) and 815 ILCS 530/45. Plaintiffs have plausibly alleged that Duly collected and then disseminated Plaintiffs’ sensitive medical information to Meta without Plaintiffs’ consent, which is enough for them to allege a negligence claim. The Court reaches this conclusion even though, as Duly points out, the Illinois

cases establishing a duty to safeguard pertained to data breaches rather than intentional transmission. The Court reaches this conclusion for the same reasons laid out in *Smith v. Loyola University Medical Center*, 2024 WL 3338941, at *7 (N.D. Ill. July 9, 2024), which addressed this exact issue. Duly's motion to dismiss Plaintiffs' state law negligence claim is therefore denied.

CONCLUSION

For the foregoing reasons, the Court denies Duly's motion to dismiss as to Plaintiffs' ECPA and negligence claims and grants it as to Plaintiffs' claim brought under the Illinois Eavesdropping Act. Plaintiffs' five withdrawn claims are also dismissed.

Dated: March 31, 2025



APRIL M. PERRY
United States District Judge