WO

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Montana Strong, et al., Plaintiffs, v. LifeStance Health Group Incorporated, Defendant.	No. CV-23-00682-PHX-KML **ORDER**

Montana Strong and Debra Yick filed this suit against LifeStance Health Group, Inc., alleging federal and state claims based on tracking technology LifeStance allegedly used on its website. LifeStance seeks dismissal of all claims but most of plaintiffs' claims are adequately pleaded. Therefore, the motion to dismiss is granted in part and denied in part. Plaintiffs' intrusion-upon-seclusion claim is dismissed without leave to amend and their other claims may proceed.

I. Factual Background

LifeStance is a mental healthcare company that offers "outpatient care services via in-person locations and telemedicine." (Doc. 32 at 5.[1]) LifeStance has 600 locations and "employs more than 5,200 psychiatrists, advance practice nurses, psychologists and therapists." (Doc. 32 at 5.) Those professionals provide treatment for conditions such as depression, PTSD, and bipolar disorder. (Doc. 32 at 22.) LifeStance markets and provides its services through a website, www.LifeStance.com. (Doc. 32 at 4.) Opting "to put its

[1] The record citations are to the pagination generated by ECF.

profits over the privacy of its Users, . . . LifeStance installed certain tracking technologies on its website in order to intercept and to send personally identifiable information ('PII') and protected health information ('PHI')[2] . . . to third parties such as Meta Platforms, Inc. d/b/a Facebook[3] . . . without the informed consent of its users." (Doc. 32 at 6.) The tracking technology central to this case is known as the "Meta Pixel," or simply "the Pixel."

The Pixel is "[i]nvisible to the naked eye" and "is a piece of code that tracks people and [the] type of actions they take as they interact with a website." (Doc. 32 at 6.) The tracked actions include "which buttons the person clicks" and "the text or phrases they type into various portions of the website." (Doc. 32 at 6.) The Pixel duplicates the user's communications and "send[s] those communications to Facebook." (Doc. 32 at 30.) This transmission to Facebook "occurs contemporaneously, invisibly and without the [user's] knowledge." (Doc. 32 at 30.) The information captured by the Pixel and sent to Facebook "is then linked to users' unique Facebook user ID . . . which allows Facebook and other third parties to personally identify those users and associates their private information with their Facebook profiles." (Doc. 32 at 6–7.)

Based on the ability to match the information the Pixel sends to Facebook with a Facebook user ID, plaintiffs claim "there is no anonymity in the information disclosed to Facebook." (Doc. 32 at 7.) According to plaintiffs, the Pixel "disclosed information that allows a third party (*e.g.*, Facebook) to know when and where a specific patient was seeking confidential medical care, for what mental health condition, and the precise care they sought or received." (Doc. 32 at 8.) "Facebook, in turn, sells users' [private information] to third-party marketers who geo-target plaintiffs' and class members' Meta accounts" based on that information. (Doc. 32 at 8.)

II. Parties and Claims

Plaintiff Montana Strong is a resident of New York, plaintiff Debra Yick is a resident of California, and LifeStance is a Delaware corporation with its principal place of

[2] This order refers to PII and PHI collectively as "private information."
[3] The parties appear to use "Facebook" and "Meta" interchangeably and the court does the same.

business in Arizona. (Doc. 32 at 15.) While in New York, Strong accessed LifeStance's website to locate mental health providers in New York, "communicate with healthcare providers, research particular medical concerns and treatments, fill out forms, [and] schedule and attend appointments." (Doc. 32 at 62-63.) While using the website, Strong also "provided her medical history and her height, weight and ethnicity." (Doc. 32 at 63.) As for Yick, she accessed the website while she was in California, and she performed similar tasks to Strong. (Doc. 32 at 64-64.) Both Strong and Yick subsequently received "targeted advertisements" on their social media accounts, including advertisements relevant to their particular mental health conditions. (Doc. 32 at 64.)

Based on LifeStance's use of the Pixel and the parties' locations, the complaint alleges claims under federal, Arizona, New York, and California law. Strong and Yick together allege a federal and Arizona state-law claim on behalf of a putative nationwide class that includes all individuals in the United States who visited the website and had their private information disclosed. Strong separately alleges a claim under New York law and seeks to represent a New York class that includes all individuals in New York who had their private information disclosed. And Yick separately alleges claims under California law and seeks to represent a California class including all individuals in California who had their private information disclosed.

The amended complaint asserts the following eight claims on behalf of the identified groups:

1. Violation of the California Invasion of Privacy Act (California class);
2. Violation of the California Confidentiality of Medical Information Act (California class);
3. Violations of Electronic Communications Privacy Act (Nationwide class);
4. Violation of California Unfair Competition Law (Unlawful Business Practices Prong) (California class);
5. Violation of the California Unfair Competition Law (Unfair Prong) (California class);

6. Violation of the Arizona Consumer Fraud Act (Nationwide class);
7. Violation of New York General Business Law (New York class);
8. Arizona Common Law Invasion of Property (Nationwide class).

In briefing the motion to dismiss, the parties grouped the analysis of similar claims together. The court does the same here.

III. Legal Standard

"To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (internal citations omitted)). This is not a "probability requirement," but a requirement that the factual allegations show "more than a sheer possibility that a defendant has acted unlawfully." *Id.* A claim is facially plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* "[D]etermining whether a complaint states a plausible claim is context specific, requiring the reviewing court to draw on its experience and common sense." *Id.* at 663–64.

IV. Wiretap Claims

Plaintiffs' sole claim under federal law is a wiretap claim under the Electronic Communications Privacy Act (the "Wiretap Act"), 18 U.S.C. § 2511(1). Yick brings a similar claim under section 931(a) of the California Invasion of Privacy Act ("CIPA"). Much of the analysis for the Wiretap Act and CIPA "is the same[.]" *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020) (quotation omitted); *see also In re Meta Pixel Healthcare Litigatio*n, 647 F. Supp. 3d 778, 798 (N.D. Cal. 2022) (analyzing Wiretap Act claim and then only analyzing defendant's additional defense under CIPA). But here, LifeStance makes certain arguments that apply only to CIPA such that it is simplest to separate the two.

A. Wiretap Act Claim

"The Wiretap Act provides a civil cause of action to 'any person whose wire, oral,

or electronic communication is intercepted, disclosed, or intentionally used in violation of [18 U.S.C. §§ 2510–2523].'" *Bliss v. CoreCivic, Inc.*, 978 F.3d 1144, 1147 (9th Cir. 2020) (quoting 18 U.S.C. § 2520(a)). LifeStance argues parties to communications (like LifeStance was here) generally cannot be held liable under the Wiretap Act and no exception to that rule applies under the facts alleged in the complaint.

Normally, a person who intercepts a "wire, oral, or electronic communication" cannot be liable under the Wiretap Act if that person was "a party to the communication." 18 U.S.C. § 2511(2)(d). But a party to a communication may be liable if the "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." *Id.* This provision that allows for a party to a communication to be found liable is often referred to as the "crime-tort exception." *R.C. v. Walgreen Co.*, No. EDCV 23-1933 JGB (SPX), 2024 WL 2263395, at *15 (C.D. Cal. May 9, 2024).

The crime-tort exception requires "the *purpose* for the interception—its intended use—[be] criminal or tortious." *Sussman v. Am. Broad. Companies, Inc.*, 186 F.3d 1200, 1202 (9th Cir. 1999). "[T]he existence of a lawful purpose does not mean that the interception is not also for a tortious or unlawful purpose." *Id.* For example, the crime-tort exception may apply when a communication was intercepted "for the purpose of committing unfair business practices." *Deteresa v. Am. Broad. Companies, Inc.*, 121 F.3d 460, 467 n.4 (9th Cir. 1997).

Plaintiffs allege the crime-tort exception applies based on various theories, including that LifeStance's interception and relaying of plaintiffs' information to Meta violated the Health Insurance Portability and Accountability Act ("HIPAA").[4] (*See* Docs. 32 at 81–82, 47 at 11.) Plaintiffs need only establish a single plausible basis to take advantage of the crime-tort exception. *See* 18 U.S.C. § 2511(2)(d) (the party exception to

[4] The complaint alleges LifeStance used the allegedly HIPAA-protected information "to improve its advertising and bolster its revenues." (Doc. 32 at 21.) That is, the purpose of the interception was to violate HIPAA to improve advertising. As recently noted in a similar case, "alleging a defendant intercepted data to use the data in violation of criminal or tort laws suffices to invoke the crime-tort exception." *Castillo v. Costco Wholesale Corp.*, No. 2:23-CV-01548-JHC, 2024 WL 4785136, at *5 (W.D. Wash. Nov. 14, 2024).

the Wiretap Act does not apply if the communication "is intercepted for the purpose of committing *any* criminal or tortious act.") (emphasis added). Thus, the wiretap claim can proceed if plaintiffs plausibly alleged LifeStance's interception was done to violate HIPAA.

HIPAA makes it a federal crime to disclose "individually identifiable health information" ("IIHI"). 42 U.S.C. § 1320d-6(a)(3). Information is IIHI if it (1) is "created or received by" a healthcare provider, (2) "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 (3) either "identifies the individual" or provides a reasonable basis to identify the individual. 42 U.S.C. § 1320d(6)(A)–(B). LifeStance argues the information allegedly disclosed through the Pixel fails all three prongs.[5] (*See* Doc. 41 at 15–17.) That is, LifeStance claims IIHI was not disclosed because (1) plaintiffs alleged Meta, not LifeStance, created and received the purported IIHI; (2) the information the Pixel purportedly transmitted to Meta does not "identif[y] or provide[ ] a reasonable basis to identify any individuals"; and (3) the information the Pixel purportedly transmitted does not qualify as related to physical or mental health. (Doc. 41 at 15–16.)

LifeStance's arguments regarding IIHI depend in part on the complaint's allegations regarding how the Pixel interacts with "cookies." Cookies "are small files of information that a web server generates and sends to a web browser" that "help inform websites about the user, enabling the websites to personalize the user experience." (Doc. 32 at 21.) The Pixel—"which is embedded in and throughout" LifeStance's website (Doc. 32 at 41)—"can access [ ] cookie[s] and send certain identifying information like the User's Facebook ID to Facebook along with the other data relating to the User's Website inputs." (Doc. 32 at 21.)

LifeStance attacks the first IIHI requirement that information be "created or

[5] LifeStance's motion does not list the second requirement that the information relate to an individual's physical or mental health or condition. (Doc. 41 at 15.) But LifeStance argues the type of information the Pixel disclosed does not qualify as IIHI, presumably an argument made based on the second requirement. (Doc. 41 at 16.)

received" by a healthcare provider by claiming "the only identifying information at issue are Facebook's cookies, which are both 'created' *and* 'received' by Facebook—not Lifestance." (Doc. 41 at 16.) In other words, LifeStance argues the purported IIHI was neither "created" nor "received" by LifeStance. LifeStance may have abandoned this exceptionally-weak argument by failing to mention it in the reply.

Assuming LifeStance has not abandoned this argument, the complaint alleges that when an individual visits the website, the Pixel tracks everything the visitor does on the website, including "which pages they view and the text or phrases they type into various portions of the website (such as a general search bar, chat feature or text box)." (Doc. 32 at 6.) After that, the Pixel tracks when visitors are waiting in telehealth waiting rooms for appointments with treatment providers, searches for which were also tracked through the Pixel. (Doc. 32 at 8.) The Pixel also has the capability to access a "Facebook-specific cookie" that includes a Facebook ID.[6] (Doc. 32 at 20.) The Pixel then "send[s] certain identifying information like the User's Facebook ID to Facebook along with the other data relating to the User's Website inputs." (Doc. 32 at 20.) Accepting the allegations as true, the Pixel captures information, packages it with information gleaned from a preexisting cookie, and transmits the combined information to Meta. Thus, identifying information is created and received by LifeStance such that the first requirement for IIHI is met.

The second requirement for IIHI is that the information must "relate[] to the past, present, or future physical or mental health or condition of an individual." 42 U.S.C. § 1320d(6)(B). LifeStance argues the "type of data that was allegedly transmitted fall[s] well short" of relating to mental or physical conditions. (Doc. 41 at 16.) According to LifeStance, the Pixel only captured and transmitted relatively banal information such as the pages a user visited. In support of this argument, LifeStance cites to *Hartley v. University of Chicago Medical Center*, No. 22-C-5891, 2023 WL 7386060, at *2 (N.D. Ill. Nov. 8, 2023). (*See* Doc. 41 at 16.) But the information allegedly transmitted in *Hartley*

[6] Plaintiffs allege Facebook IDs "allow[ ] Facebook and other third parties to personally identify [ ] those Users and associate[ ] their Private Information with their Facebook profiles." (Doc. 32 at 6–7.)

appears to have been more limited than what was transmitted in the present case.

The plaintiffs in *Hartley* brought a Wiretap Act claim against their healthcare provider which maintained a website to communicate with its patients. *Id.* at *1. The plaintiffs alleged their IIHI had been transmitted to Facebook via the Pixel and the plaintiffs invoked the crime-tort exception. *Id.* The information allegedly transmitted was the plaintiffs' "IP addresses, Facebook IDs, cookie identifiers, device identifiers and account numbers and the contents of thee [sic] communications, *i.e.*, 'URLs, buttons, pages, and tabs they click and view.'" *Hartley*, 2023 WL 7386060, at *2. The *Hartley* court concluded that information did not qualify as IIHI because the plaintiffs had failed to allege "any particular health or treatment information disclosure specific as to them that [the defendant] allegedly made" to a third party. *Id.* (citation omitted).

The disclosures alleged in *Hartley* are different from those alleged here, as plaintiffs make clear. (*See* Doc. 47 at 18.) In the present case, the Pixel operated to disclose plaintiffs' "specific health conditions" which they included in a sealed version of their complaint. Plaintiffs also alleged the disclosure of their "communicat[ions] with healthcare providers, [their] researching [of] particular medical concerns and treatments," and their "performing [of] other tasks related to their specific medical inquires and treatment." (Doc. 47 at 18 (citing Doc. 32).) Unlike *Hartley*, plaintiffs' allegations are not merely "generalizations as to what [defendant] was communicating to Facebook." *Id.* Thus, the type of data the Pixel allegedly transmitted in this case plausibly qualifies as the type of data protected by HIPAA.

Finally, LifeStance argues the information was not IIHI because it did not identify the individual or provide a reasonable basis to identify the individual. 42 U.S.C. § 1320d(6)(B). But plaintiffs allege the information LifeStance transmitted to Meta included their "name and email, their medical conditions, treatment and/or specific providers," and "Facebook IDs, IP addresses and/or device IDs." (Doc. 32 at 41, 44.) It is difficult to understand what more LifeStance believes would be necessary for information to be identifying.

The complaint alleges the Pixel deployed by LifeStance captured information received by LifeStance and then packaged it with cookies created by Facebook to transmit both the medical information and identifying information to Facebook. Based on these allegations, plaintiffs sufficiently pleaded LifeStance received and disclosed IIHI. Accordingly, plaintiffs plausibly pleaded LifeStance intercepted the communications for the purpose of violating HIPAA. LifeStance has not argued that a violation of HIPAA would not be sufficient to invoke the crime-tort exception and other district courts analyzing similar allegations have held otherwise. *See Castillo v. Costco Wholesale Corp.*, No. 2:23-CV-01548-JHC, 2024 WL 4785136, at *7 (W.D. Wash. Nov. 14, 2024); *Kurowski v. Rush Sys. for Health*, No. 22C5380, 2023 WL 8544084, at *2-*3 (N.D. Ill. Dec. 11, 2023). The request to dismiss plaintiffs' Wiretap Act claim is denied.

B. California Invasion of Privacy Act ("CIPA") Claim

LifeStance seeks dismissal of plaintiffs' CIPA claim arguing: (1) CIPA's first clause does not apply to internet communications; (2) any communication of plaintiffs' information to Meta using a non-Pixel method mentioned in the complaint is not actionable under CIPA; (3) plaintiffs do not sufficiently allege data was sent, received, or intercepted in California; and (4) plaintiffs fail to adequately allege LifeStance aided or abetted wrongdoing by Meta.[7] (*See* Doc. 41 at 19–23.) None of these arguments succeed.

Courts have interpreted the relevant provision of CIPA, Cal. Penal Code § 631(a), as containing two clauses that apply to different situations.[8] The "first clause" of that provision has been interpreted as "applying only to communications over telephones and

[7] LifeStance also argues it is exempt from CIPA because the same party exception that applies to the Wiretap Act applies to CIPA. (Doc. 41 at 20, 21.) But LifeStance recognizes the crime-tort exception recognized in federal law would apply to CIPA as well. Because the crime-tort exception applies to the federal claim here, there is no need to analyze that argument separately under CIPA. (*See* Doc. 41 at 20.)

[8] The first clause creates liability for "any person who by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system[.]" Cal. Penal Code § 631(a). The second clause creates liability for individuals who "read[ ] or attempt[ ] to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable, or is being sent from, or received at any place within this state[.]" *Id.*

not through the internet." *Licea v. Am. Eagle Outfitters, Inc.*, 659 F. Supp. 3d 1072, 1079 (C.D. Cal. 2023). But CIPA's second clause indisputably applies to internet communications. *See, e.g.*, *Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, Section 631(a) applies to Internet communications."). Plaintiffs rely only on the second clause, as they make abundantly clear by quoting CIPA in the complaint but omitting the first clause. (Doc. 32 at 74.) LifeStance's argument regarding the applicability of the first clause is irrelevant. (Doc. 41 at 20.)

LifeStance's second argument aimed at the CIPA claim is that any sharing of plaintiffs' information with Meta is not actionable to the extent the claim is based on CAPI, a non-Pixel technology mentioned in the complaint. (Doc. 41 at 21.) According to LifeStance, CAPI involves a "two-step process" of LifeStance "record[ing] its own communications and then shar[ing] those recordings" with Meta. (*See* Doc. 41 at 21.) Even assuming this is how CAPI operated, this argument fails at the motion-to-dismiss stage. (*See* Doc. 41 at 21.)

LifeStance may be correct that it did not violate CIPA if only CAPI technology is at issue. That is, if the transmission of information to Meta only occurred after LifeStance already received the information from the plaintiffs, rather than contemporaneously, CIPA may not apply. *See Graham v. Noom*, 533 F. Supp. 3d 823, 831 (N.D. Cal. 2021) ("Under CIPA, a party to a communication does not violate the statute where it records its own communications and then shares those recordings."). But the court need not wade into this issue because CAPI is merely an alternative basis for the CIPA claim. Thus, the CIPA claim based on the Pixel's alleged simultaneous transmission can proceed regardless of whether CAPI was also used.

LifeStance's third argument for dismissing the CIPA claim is the complaint does not allege plaintiffs' information was "sent from[ ] or received at any place within [California]." (Doc. 41 at 22 (citing Cal. Penal Code § 631(a).) Plaintiffs allege repeatedly that some of the relevant conduct occurred in California. (*See* Doc. 32 at 15, 66–68, 74

(establishing Yick was in California at all relevant times and that the "communications were intercepted in California where Meta is located.").) That is sufficient.

LifeStance's final argument involves what one court labeled the "fourth prong" of CIPA. *Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 897 (N.D. Cal. 2023) (citing Cal. Penal Code § 631(a)(4)). Under that prong, LifeStance may be liable if it aided and abetted violations of CIPA by Facebook. LifeStance seems to argue it cannot be liable under this theory because the complaint does not identify any wrongdoing by Facebook. But plaintiffs have alleged LifeStance worked with Facebook to surveil visitors to the LifeStance website to provide confidential information that Facebook then used itself, by selling it "to third-party marketers who geo-target plaintiffs' and class members' Meta account." (Doc. 32 at 8; *See also* Doc. 32 at 75 (LifeStance "intentionally inserted an electronic device that, without the knowledge and consent of Plaintiffs and Class members, recorded and transmitted their confidential communications with [LifeStance] to a third party."); Doc. 32 at 74 (LifeStance "aided, employed, agreed with, and conspired with [Meta] and [other third parties] to track and intercept Plaintiffs' and Class Members' internet communications while using [LifeStance's] Website.").) As explained by another court, "if a third party listens in on a conversation between the participants (even if one participant consents to the presence of that third party), then the third party is liable under the second prong [of § 631] (and the participant is often liable under the fourth prong)." *Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 897–98 (N.D. Cal. 2023).[9]

Taking plaintiffs' well-pleaded facts as true, LifeStance's arguments against the CIPA claim fails and its motion to dismiss the claim is denied.

V. Unfair Competition Claims

Yick alleges violations of the unfair and unlawful business practices prong of

[9] LifeStance argues it cannot be liable under an aiding and abetting theory because of the reasoning in *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 831–32 (N.D. Cal. 2021). But *Javier* rejects the reasoning in *Graham* as inconsistent with the statutory text and guidance from the California Supreme Court. *Javier*, 649 F. Supp. 3d at 900. The reasoning of *Javier* is more persuasive. The allegations in the current case cast Facebook not as merely providing software, such as the software vendor in *Graham*, but as a third-party that used the data for itself, such as the software vendor at issue in *Revitch v. New Moosejaw, LLC*, No. 18-CV-06827-VC, 2019 WL 5485330, at *1 (N.D. Cal. Oct. 23, 2019).

California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, et seq. Strong alleges a claim under Arizona's Consumer Fraud Act ("AZCFA"), A.R.S. § 44-1522. Although the complaint does not make entirely clear the analytical basis for these claims, plaintiffs' opposition to the motion to dismiss states they are based on omissions and not misrepresentations. (Doc. 47 at 26 ("Plaintiff Yick premises her UCL claims on LifeStance's omissions"); Doc. 47 at 29 ("Plaintiffs Plead AZCFA Claims Based on Material Omissions").)

A. California Unfair Competition Claims

California's UCL provides a cause of action for business practices that are (1) unlawful, (2) unfair, or (3) fraudulent. Cal. Bus. & Prof. Code § 17200, *et seq*. Plaintiffs bring claims under the unlawful and unfair prongs (*see* Doc. 32 at 84–89), with the claims under both prongs centering on alleged omissions. In particular, Yick's opposition specifies the omissions were LifeStance's "failure to disclose that it embedded tracking technologies on its Website in order to collect and to disclose [private information] to third parties without informed consent." (Doc. 47 at 26.)

UCL claims based on nondisclosure like Yick's are subject to Rule 9(b)'s particularity standard. *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1127 (9th Cir. 2009). This requires allegations identifying the "the who, what, when, where, and how of the misconduct charged." *Id.* at 1124 (quotation marks and citation omitted). This particularity standard applies to the requirement that Yick plead "actual reliance on the . . . omissions at issue." *Great Pac. Sec. v. Barclays Cap., Inc.*, 743 F. App'x 780, 783 (9th Cir. 2018); *see also Durell v. Sharp Healthcare*, 108 Cal. Rptr. 3d 682, 694 (Cal. Ct. App. 2010) (discussing "actual reliance" under the "unlawful" prong of UCL). But these pleading requirements are somewhat "relaxed in fraudulent omission cases." *Short v. Hyundai Motor Co.*, 444 F. Supp. 3d 1267, 1279 (W.D. Wash. 2020). This relaxed approach is necessary because "a plaintiff in a fraud by omission suit will not be able to specify the time, place, and specific content of an omission as precisely as would a plaintiff in a false representation claim." *Falk v. Gen. Motors Corp.*, 496 F. Supp. 2d 1088, 1098–99 (N.D.

Cal. 2007).

LifeStance presents three arguments in seeking dismissal of the UCL claims. First, there are no allegations that a violation occurred in California. Second, Yick did not plead actual reliance. And third, Yick did not plead any injury. (Doc. 41 at 24-26.) None of these arguments is persuasive.

As previously noted in discussing the CIPA claim, there are numerous allegations that some of the relevant conduct occurred in California. (*See* Doc. 32 at 15, 66–68, 74 (establishing Yick was in California at all relevant times and that the "communications were intercepted in California where Meta is located.").) Those allegations are sufficient for purposes of the UCL claims.

LifeStance next contends Yick has not alleged she "actually relied" on any omissions. (Doc. 41 at 24.) According to LifeStance, Yick needed to allege she "read, understood, and actually relied on the" omissions. (Doc. 41 at 24.) Yick did allege she "viewed and relied" upon LifeStance's "privacy policies concerning the confidentiality of information provided by patients." (Doc. 32 at 86.) But LifeStance claims those allegations are not enough because Yick did not allege she "*read* LifeStance's Privacy Policy." (Doc. 48 at 11.) Construed in the light most favorable to Yick, the allegations that she "viewed and relied" on the policy include that she read the policy. Yick has adequately alleged actual reliance.

Finally, LifeStance argues Yick has not alleged she "suffered any actual injury as a result of any purported violation of the UCL." (Doc. 41 at 25.) Yick responds she suffered "loss of benefit of the bargain," (Doc. 47 at 27), because she "lost money or property" in the form of "payments to Defendant." (Doc. 32 at 87.) "[A] plaintiff who has surrender[ed] in a transaction more, or acquire[d] in a transaction less, than he or she otherwise would have may bring a UCL claim." *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 985 (N.D. Cal. 2016) (quotation marks and citation omitted). Construed in the light most favorable to Yick, she has alleged she suffered "benefit of the bargain" damages by paying

more than she otherwise would have paid.[10] That is sufficient.

B. Arizona Consumer Fraud Claim

Plaintiffs' claim under the Arizona Consumer Fraud Act ("ACFA") is also based on LifeStance failing "to disclose its use of tracking technologies." (Doc. 47 at 29.) ACFA prohibits

> [t]he act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby.

A.R.S. § 44-1522(A). As with the UCL claims, Rule 9(b)'s particularity standard applies to an ACFA claim. *Physicians Surgery Ctr. of Chandler v. Cigna Healthcare Inc.*, 609 F. Supp. 3d 930, 941 (D. Ariz. 2022) (noting Arizona's consumer fraud statute is subject to Rule 9(b)'s particularity requirements).

Plaintiffs based their ACFA claim on allegations they "viewed and relied upon [LifeStance's] representations in its privacy policies concerning the confidentiality of information [they] provided" to LifeStance, but those privacy policies contained material omissions in violation of the ACFA. (Doc. 32 at 86.) LifeStance seeks dismissal of this claim on a variety of grounds, none of which has merit.

"A claim under the ACFA's omission clause requires proof that the omission is material and made with intent that a consumer rely thereon." *Cheatham v. ADT Corp.*, 161 F. Supp. 3d 815, 830 (D. Ariz. 2016). According to LifeStance, plaintiffs have not alleged LifeStance "'intended' to make any omission upon which a consumer would rely." (Doc.

[10] LifeStance argues Yick's allegations are insufficient because she has not alleged she "paid any money to LifeStance for the protection of [her] data from disclosure, rather than for the procurement of services." (Doc. 48 at 12.) While not developed, LifeStance appears to be arguing "benefit of the bargain" damages are only appropriate when plaintiffs who purchase a service make a separate payment for "protection of their data from disclosure." LifeStance has not cited any authority imposing such a requirement and no such requirement is appropriate. *See, e.g.*, *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1072 (N.D. Cal. 2012) (finding injury based on "the allegedly overinflated cost of [a device] as a result of the false statements regarding the . . . features of the device").

41 at 29.) The complaint alleges LifeStance's omissions violated industry standards, such as the American Medical Association's Code of Medical Ethics and FTC data security guidelines. (Doc. 32 at 53-54.) LifeStance's omissions also allegedly were contrary to consumers' "general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential" and LifeStance's own privacy policies, which reflect these principles. (Doc. 32 at 48, 95.) Allegations that LifeStance acted contrary to broadly accepted standards and expectations are a sufficient basis to infer LifeStance intended for consumer to rely upon the omissions. That is, it is plausible LifeStance knew that disclosing its practices would be harmful to its business so it intentionally chose not to disclose those practices. In doing so, LifeStance plausibly intended for consumer to rely on the non-disclosure.

LifeStance's next argument is plaintiffs have not alleged "an underlying sale or advertisement of [services] as required under ACFA."[11] (Doc. 41 at 30.) The complaint alleges plaintiffs started receiving services from LifeStance in March and June 2022 and continued to receive those services until early 2023. (Doc. 32 at 63, 65.) LifeStance argues this is not sufficiently specific and plaintiffs were required to identify the "specific transaction" underlying their claim. (Doc. 41 at 30.) Given the relaxed pleading standard for omissions, the present allegations are sufficient. LifeStance is aware of the exact dates plaintiffs received services and requiring plaintiffs amend the complaint to list those dates would have no utility.

Finally, LifeStance argues plaintiffs have not alleged they suffered a cognizable injury. But as with the UCL claims, plaintiffs have alleged they "would not have used [LifeStance's] services" if they had known LifeStance was using the Pixel. (Doc. 32 at 86.) In these circumstances, the payment of any amount to LifeStance is a cognizable injury. *See Cheatham*, 161 F. Supp. 3d at 831 ((D. Ariz. 2016) (plaintiff alleged cognizable injury because she alleged "she would not have purchased her wireless security system but for [the] violation of the ACFA"). Plaintiffs' ACFA claim may proceed.

[11] ACFA defines "merchandise" as including "services." A.R.S. § 44-1521(5).

VI. New York General Business Law

Strong alleges LifeStance violated New York General Business Law ("NYGBL") § 349 which prohibits deceptive acts or practices. To state such a claim a plaintiff must allege (1) the defendant's conduct was consumer-oriented; (2) the defendant's act or practice was deceptive or misleading in a material way; and (3) the plaintiff suffered an injury as a result of the deception. *Kane v. Univ. of Rochester*, No. 23-CV-6027-FPG, 2024 WL 1178340, at *16 (W.D.N.Y. Mar. 19, 2024) (simplified) (citing NYGBL § 349(h)).

Strong's claim is based on conduct relating to LifeStance's handling of plaintiffs' private information. (Doc. 32 at 92–94.) She claims LifeStance promised to maintain the privacy and security of her private information but failed to do so, installed and used the Pixel which transmitted her private information to Facebook without her knowledge, consent, or authorization, and failed to disclose or omitted material facts about this data-sharing in its privacy policies. (Doc. 32 at 92–94.) LifeStance was allegedly aware that Strong "depended and relied upon it to keep their communications confidential," but it still disclosed her private information to Facebook. (Doc. 32 at 93.)

LifeStance presents two arguments to dismiss the NYGBL § 349 claim. First, the law does not apply to transactions or deceptions that occurred outside New York. (Doc. 41 at 32.) Second, Strong "cannot plausibly show any actual injury as a result of any alleged material deceptive act or omission." (Doc. 41 at 32, 33.) Neither argument is persuasive.

Strong alleges she resided in New York "at all relevant times[,]" including when she accessed and received healthcare services through the LifeStance website. (Doc. 32 at 15.) *See Goshen v. Mut. Life Ins. Co. of New York*, 774 N.E.2d 1190, 1195 (N.Y. 2002) (holding NYGBL § 349 requires "the deception of a consumer . . . occur in New York"). LifeStance has not cited any authority that a transaction conducted between an out-of-state entity and a New York resident, while that individual is in New York, is not subject to NYGBL § 349.

LifeStance's second argument is that Strong has not alleged a sufficient injury. "Lost benefit of the bargain is a viable theory of injury under GBL § 349." *Kane*, 2024 WL

1178340, at *17. Allegations that a consumer "would not have purchased" a particular service are sufficient under this theory. *Id.* Here, Strong alleges she expected her communications would remain confidential, she "never consented to the disclosure" of her information, and that disclosure breached her privacy. (Doc. 32 at 64-65.) Although a close call, construed in the light most favorable to Strong, those allegations plausibly establish Strong would not have used LifeStance's website if she had been aware her information would be disclosed. Thus, Strong has alleged she lost the benefit of the bargain and her NYGBL claim may proceed.

VII. Privacy Claims

A. California Confidentiality of Medical Information Act ("CMIA")

LifeStance argues plaintiffs have not adequately alleged a CMIA claim because the private information LifeStance shared with Meta was not "medical information" and it did not violate the CMIA for LifeStance to share information with Meta "to help [LifeStance] analyze data." (*See* Doc. 41 at 33–35.) LifeStance is incorrect.

Under the CMIA, "medical information" is "any individually identifiable information,[12] in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental health application information, mental or physical condition, or treatment." Cal. Civ. Code. § 56.05(i).[13] LifeStance argues plaintiffs "do not allege the disclosure of substantive information regarding medical treatment, condition, or history in anything more than conclusory fashion, and their own factual allegations

[12] "'Individually identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual." Cal. Civ. Code. § 56.05(j).

[13] LifeStance argues the CMIA only applied to mental health care after January 1, 2023. (Doc. 41 at 36.) It relies on California Assembly Bill 2089, which added "mental health application information" to the definition of "medical information" in the CMIA. (Doc. 41 at 36.) Plaintiffs respond by citing Cal. Civ. Code. § 56.05, which defined medical information as including "a patient's medical history, mental or physical condition, or treatment," (Doc. 47 at 37), and applied during the entirety of the conduct alleged here. Because Cal. Civ. Code. § 56.05 included mental conditions and treatment before any amendments and LifeStance cites no cases to the contrary, its argument fails.

demonstrate that any disclosures do not amount to medical information under [the] CMIA." (Doc. 41 at 34.) LifeStance acknowledges that plaintiffs allege disclosure of patients joining a waiting room to meet with a provider, patients clicking to select which state they are in during their appointment, patients' searches for therapists, patients' calls to therapists, and patients "access[ing] and review[ing] conditions treated by LifeStance[.]" But LifeStance argues the CMIA only protects "substantive information regarding a patient's medical condition or history." (Doc. 41 at 34.)

LifeStance cites three cases to support its contention that what it shared with Meta was not medical information. *See Cousin v. Sharp Healthcare*, 681 F. Supp. 3d 1117, 1124 (S.D. Cal. 2023); *Wilson v. Rater8, LLC*, 20-cv-1515-DMS-LL, 2021 WL 4865930, at *4–5 (S.D. Cal. 2021); *Eisenhower Medical Center v. Superior Court*, 226 Cal. App. 4th 430, 435 (2014). These cases do not support LifeStance's argument.

In *Cousin*, which also concerned the Pixel, the court initially determined plaintiffs' medical information disclosure allegations were "conclusory and devoid of any factual support." 681 F. Supp. 3d at 1123. The medical information plaintiffs alleged to have been shared was their "browsing activity" of researching doctors, looking for providers, and searching for medical specialists. *Id.* at 1124. The court held that was not protected health information and dismissed plaintiffs' CMIA claim. *Id.* at 1124. But the court later reversed course based on additional allegations, including that defendants shared plaintiffs' searches for "their particular medical conditions" and their use of "[d]efendant's website [to search] for doctors who specialized in these conditions and for information about their conditions." *See Cousin v. Sharp Healthcare*, 702 F. Supp. 3d 967, 972–73 (S.D. Cal. 2023). Based on the additional allegations, the court denied defendants' motion to dismiss. *Id.* Plaintiffs alleged far more here than the court initially dismissed in *Cousins*. Among other allegations, plaintiffs have plausibly pleaded that LifeStance shared their "medical information"—like "the type of medical treatments [they] sought," and their "medical conditions"—with Facebook along with the fact that they were waiting for specific providers in an online room (and therefore presumably a patient of a LifeStance mental

health provider). (Doc. 47 at 34.)

In *Wilson*, the plaintiff alleged the defendant disclosed his "name, cellular telephone number, treating physician names, medical treatment appointment information, and medical treatment discharge dates and times" which the court determined was not "medical information." 2021 WL 4865930, at *5. Here too, however, plaintiffs have alleged far more personal medical information than that in *Wilson*, including the types of treatment sought for specific mental health complaints. (*See* Doc. 47 at 34.) Similarly, in *Eisenhower*, plaintiffs had only alleged the information disclosed was their "name, medical record number [ ], age, date of birth, and last four digits of the person's Social Security number." 226 Cal. App. 4th at 166. The court found this was not "medical information" but recognized that "medical history, mental or physical condition, or treatment of the individual" is "medical information." *Id.* at 170. That is the type of information plaintiffs have alleged was disclosed here. LifeStance's argument that it did not share "medical information" with Facebook fails.

LifeStance also argues the "CMIA expressly allows health-care providers to rely upon third parties, like Meta, to help analyze data" like that alleged here. (Doc. 41 at 35.) It cites to section 56.10(c) of the CMIA which allows medical information to be disclosed "to a person or entity that provides billing, claims management, medical data processing, or other administrative services for providers of health care." (Doc. 41 at 36.) But plaintiffs have alleged LifeStance shares their medical information "for purely commercial ends, *i.e.* marketing and advertising by LifeStance, Meta, and other unauthorized third parties." (*See* Doc. 47 at 36.) Meta cannot plausibly be compared to a provider of "administrative services" like a billing company. Plaintiffs' CMIA claim may proceed.

B. Invasion of Privacy – Intrusion Upon Seclusion

Plaintiffs allege an Arizona common law claim for intrusion upon seclusion. According to plaintiffs, LifeStance violated their privacy by disclosing their sensitive medical and personally identifiable information to third parties without their consent. (Doc. 32 at 95.) They contend that this information was intended solely for LifeStance and was

to remain confidential, asserting its unauthorized disclosure "is highly offensive to the reasonable person." (Doc. 32 at 95.) Plaintiffs believe they had a reasonable expectation of privacy based on LifeStance's privacy policy, which assured them of confidentiality and protection against unauthorized disclosures to third parties. (Doc. 32 at 95.)

Arizona follows the Second Restatement's definition of intrusion upon seclusion. Under that definition, one who "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." *Hart v. Seven Resorts Inc.*, 947 P.2d 846, 853 (Ariz. Ct. App. 1997) (quoting Restatement (Second) of Torts § 652B). LifeStance argues plaintiffs "cannot allege that there was an 'intentional intrusion' on the part of Lifestance" because it "had a right to know [plaintiffs'] private information because [plaintiffs] allege that they voluntarily disclosed that information and communicated it directly to LifeStance." (Doc. 41 at 37.) LifeStance is correct.

As LifeStance points out, another case from this court discussed a similar situation. In *Bruer v. Phillips Law Group PC*, the plaintiff claimed invasion of privacy based on information that she had given to the defendant and which the defendant later sent back to her. No. CV-18-01843-PHX-JJT, 2019 WL 2552060, at *1 (D. Ariz. June 20, 2019). She complained that the file contained sensitive personal information that the defendant sent to her without "applying required redactions" or including "password protection" on the file. *Id.* The court dismissed the intrusion-upon-seclusion claim because the defendants obtained the plaintiff's "information [with her] permission" so she "[did] not plausibly allege[ ] an invasion of privacy." *Id.* at *3.

Here, there is no dispute that the plaintiffs voluntarily gave LifeStance their personal information. Plaintiffs cite a California Pixel case which allowed an intrusion-upon-seclusion case to move forward, but the plaintiffs in that case were suing Meta because they had *not* voluntarily given their information to it. *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 778. Here, plaintiffs are suing LifeStance, to whom they did voluntarily

give their information. Plaintiffs' intrusion-upon-seclusion claim is dismissed without leave to amend.

VIII. Conclusion

Plaintiffs' intrusion-upon-seclusion claim is dismissed without leave to amend but all their other claims may proceed. Because of the age of this case, the parties must immediately prepare and prepare their Rule 26(f) report. In discussing case management dates, the parties must set the deadline for dispositive motions no later than April 2026.

Accordingly,

IT IS ORDERED the Motion to Dismiss (Doc. 41) is **GRANTED IN PART and DENIED IN PART**.

IT IS FURTHER ORDERED as follows:

The parties are directed to meet, confer, and develop a Rule 26(f) Joint Case Management Report, which must be filed **within 2 weeks of the date of this order**. It is the responsibility of plaintiff(s) to initiate the Rule 26(f) meeting and prepare the Joint Case Management Report. Defendant(s) shall promptly and cooperatively participate in the Rule 26(f) meeting and assist in preparation of the Joint Case Management Report.

The Joint Case Management Report shall contain the following information in separately-numbered paragraphs.

1. The parties who attended the Rule 26(f) meeting and assisted in developing the Joint Case Management Report;
2. A list of all parties in the case, including any parent corporations or entities (for recusal purposes);
3. Any parties that have not been served and an explanation of why they have not been served, and any parties that have been served but have not answered or otherwise appeared;
4. A statement of whether any party expects to add additional parties to the case or otherwise amend pleadings;
5. The names of any parties not subject to the Court's personal (or *in rem*)

jurisdiction;

6. A description of the basis for the Court's subject matter jurisdiction, citing specific jurisdictional statutes. If jurisdiction is based on diversity of citizenship, the report shall include a statement of the citizenship of every party and a description of the amount in dispute. *See* 28 U.S.C. §1332;

7. A short statement of the nature of the case (no more than three pages), including a description of each claim, defense, and affirmative defense;

8. A listing of contemplated motions and a statement of the issues to be decided by those motions;

9. Whether the case is suitable for reassignment to a United States Magistrate Judge for all purposes or suitable for referral to a United States Magistrate Judge for a settlement conference;

10. The status of any related cases pending before this or other courts;

11. A discussion of any issues relating to preservation, disclosure, or discovery of electronically stored information ("ESI"), including the parties' preservation of ESI and the form or forms in which it will be produced;

12. A discussion of any issues relating to claims of privilege or work product;

13. A discussion of necessary discovery, which should take into account the December 1, 2015 amendments to Rule 26(b)(1) and should include:

    a. The extent, nature, and location of discovery anticipated by the parties and why it is proportional to the needs of the case;

    b. Suggested changes, if any, to the discovery limitations imposed by the Federal Rules of Civil Procedure;

    c. The number of hours permitted for each deposition. The parties also should consider whether a total number of deposition hours should be set in the case, such as twenty total hours for plaintiffs and twenty total hours for defendants. Such overall time limits have the advantage of providing an incentive for each side to be as efficient as possible in

each deposition, while also allowing parties to allocate time among witnesses depending on the importance and complexity of subjects to be covered with the witnesses;

14. Proposed deadlines for each of the following events. In proposing deadlines, the parties should keep in mind the Case Management Order will contain deadlines to govern this case and once the dates have been set the Court will vary them only upon a showing of good cause. A request by counsel for extension of discovery deadlines in any case that has been pending more than two years must be accompanied by a certification stating the client is aware of and approves of the requested extension. The Court does not consider settlement talks or the scheduling of mediations to constitute good cause for an extension. The parties must propose the following:

a. A deadline for the completion of fact discovery, which will also be the deadline for pretrial disclosures pursuant to Rule 26(a)(3). This deadline is the date by which all fact discovery must be *completed*. Discovery requests must be served and depositions noticed sufficiently in advance of this date to ensure reasonable completion by the deadline, including time to resolve discovery disputes. Absent extraordinary circumstances, the Court will not entertain discovery disputes after this deadline;

b. Dates for full and complete expert disclosures and rebuttal expert disclosures, if any;

c. A deadline for completion of all expert depositions;

d. A date by which any Rule 35 physical or mental examination will be noticed if such an examination is required by any issues in the case;

e. A deadline for filing dispositive motions;

f. Case-specific deadlines and dates, such as the deadline to file a motion for class certification or a date on which the parties are available for a

Markman (patent claim construction) hearing;

g. A date by which the parties shall have engaged in face-to-face good faith settlement talks;

h. Whether a jury trial has been requested and whether the request for a jury trial is contested, setting forth the reasons if the request is contested;

i. Any other matters that will aid the Court and parties in resolving this case in a just, speedy, and inexpensive manner as required by Federal Rule of Civil Procedure 1;

15. A statement indicating whether the parties would prefer that the Court hold a case management conference before issuing a scheduling order—and, if so, an explanation of why the conference would be helpful.

IT IS FURTHER ORDERED the parties shall file a proposed Case Management Order containing all the proposed dates at the same time they file the Rule 26(f) Case Management Report. The proposed Case Management Order must also be emailed in Word format to Lanham_chambers@azd.uscourts.gov.

Dated this 27th day of January, 2025.

Krissa M. Lanham

Honorable Krissa M. Lanham
United States District Judge