UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

EMMA DAWSON, et al.,

Plaintiffs,

v.

META PLATFORMS, INC., et al.,

Defendants.

Case No. 26-cv-00751-RFL

ORDER GRANTING MOTION TO DISMISS AND DENYING MOTION FOR SANCTIONS

Re: Dkt. Nos. 29, 38

I. INTRODUCTION

Plaintiffs filed this putative class action against Defendants Meta Platforms, Inc., and WhatsApp LLC, alleging that Meta and WhatsApp store and can access WhatsApp users' communications despite representing to users that communications on WhatsApp are private and fully encrypted. (Dkt. No. 1. ("Compl.").) The complaint relies principally on allegations from unspecified whistleblowers to assert that Meta employees are indeed able to access users' WhatsApp messages. Defendants move to dismiss the complaint and for sanctions under Federal Rule of Civil Procedure 11. (Dkt. Nos. 29, 38.) As explained further below, contrary to Defendants' view, most of the allegations are not subject to the heightened pleading requirements for fraud. But at the same time, there is still insufficient information in the complaint about the basis for the whistleblowers' knowledge for the claims to be viable as currently pled. Though Plaintiffs need not identify the whistleblowers to plead a plausible basis for their claims, they do need to provide some facts supporting an inference that the whistleblowers have firsthand knowledge or some other reliable basis for their accusations. The motion to dismiss is **GRANTED** with leave to amend, and the motion for sanctions is **DENIED**.

II. BACKGROUND

The facts detailed below are based on the allegations contained in the operative complaint, the truth of which the Court accepts for purposes of resolving the motion to dismiss. *See Boquist v. Courtney*, 32 F.4th 764, 772 (9th Cir. 2022).

A. WhatsApp and Its Privacy Representations

WhatsApp is "the most popular messaging app in the world," "purport[ing] to offer its more than three billion users in over 180 countries privacy, security and peace of mind" through representations regarding its security and privacy features. (Compl. ¶ 1.) Two "important promises" on WhatsApp's website are illustrative. (*Id.*) First, WhatsApp advertises that it is "encrypted for everyone" and allows users to "message privately with everyone." (*Id.* (cleaned up).) Second, WhatsApp claims that it "does not store messages once they are delivered." (*Id.*)

Other representations regarding WhatsApp's purported privacy features abound. For instance, on its "Privacy" page, WhatsApp's website highlights that "with end-to-end encryption[1] on WhatsApp, your personal messages, photos, calls and more stay between you and the people you choose, meaning not even WhatsApp can see them." (*Id.* ¶ 24 (cleaned up).) As another example, WhatsApp's "FAQ" page claims that "not even WhatsApp can read, listen to, or share users' personal images and calls" and that end-to-end encryption occurs "automatically." (*Id.* ¶ 26 (cleaned up).) As yet another example, WhatsApp chats have a disclaimer at the top: "Messages and calls are end-to-end encrypted. Only people in this chat can read, listen to, or share them." (*Id.* ¶ 27.)

WhatsApp represents that messages can be read by individuals who are not the sender or recipient(s) in only limited circumstances. First, WhatsApp discloses that when a user reports another user in an individual chat or reports abuse in a group chat, WhatsApp receives up to five of the last messages sent to the reporting user and basic information about the last five calls that took place. (*Id.* ¶ 28.) Second, when users contact WhatsApp for customer support, "they may

[1] End-to-end encryption "is a method of securing digital communications wherein data is encrypted on the sender's device and only decrypted once it reaches the recipient's device." (*Id.* ¶ 32.)

provide WhatsApp with information 'including copies of [their] messages.'" (*Id.* ¶ 29.) Third, WhatsApp identifies certain uses cases in which WhatsApp and Meta can see users' messages including "business messaging services" and "communications that are not encrypted (such as communications with Meta services or communications with businesses using Cloud API[])." (*Id.* ¶ 30.) Finally, WhatsApp discloses that it "may collect, use, preserve, and share user information if [it has] a good-faith belief that it is reasonably necessary to (a) keep [its] users safe, (b) detect, investigate, and prevent illegal activity, (c) respond to legal process, or to government requests, [and] (d) enforce [its] Terms and policies." (*Id.* ¶ 31.) However, in that same disclosure, WhatsApp reaffirms, "We also offer end-to-end encryption for our services, which is always activated. End-to-end encryption means that messages are encrypted to protect against WhatsApp and third parties from reading them." (*Id.*)

B. WhatsApp and Meta's Access of Users' Encrypted Communications

According to alleged unspecified whistleblowers, Meta and WhatsApp's representations that they do not have access to the substance of users' communications on WhatsApp are false. "As the whistleblowers here have explained":

> WhatsApp and Meta store and have unlimited access to WhatsApp encrypted communications, and the process for Meta workers to obtain that access is quite simple. A worker need only send a "task" (*i.e.*, request via Meta's internal system) to a Meta engineer with an explanation that they need access to WhatsApp messages for their job. The Meta engineering team will then grant access—often without any scrutiny at all—and the worker's workstation will then have a new window or widget available that can pull up any WhatsApp user's messages based on the user's User ID number, which is unique to a user but identical across all Meta products.
>
> Once the Meta worker has this access, they can read users' messages by opening the widget; no separate decryption step is required. The WhatsApp messages appear in widgets commingled with widgets containing messages from unencrypted sources. Messages appear almost as soon as they are communicated—essentially, in real-time. Moreover, access is unlimited in temporal scope, with Meta workers able to access messages from the time users first activated their accounts, including those messages users believe they have deleted.
>
> Some users—such as certain celebrities, politicians, and Meta employees—are afforded special handling by Meta such that

> access to their encrypted messages is more closely tracked within Meta and WhatsApp. Meta workers still have access to these users' messages, but their access of the accounts flags the worker for investigation. Even as to these privileged few WhatsApp users, however, Meta and WhatsApp are still misleading them and violating their privacy by storing their supposedly private, end-to-end encrypted, messages.
>
> Although Meta has kept the circle on its fraud small, it has not kept it small enough. It attempted to prevent dissemination of this information by heavily siloing workers in different groups and telling them to "stay in [their] lane" when and if they started to piece together the truth. As discussed below, Meta also actively misrepresented the facts about its access and storage when journalists came close to discovering the truth. Meta has also tried to prevent the truth from coming out by imposing onerous nondisclosure agreements on its workers, essentially threatening the full force of one of the world's richest companies if any of these individuals dared reveal what goes on behind closed doors at the company. These efforts have now failed, but they worked for many, many years by obscuring the truth.

(*Id*. ¶¶ 36–39.)

C. This Case

Plaintiffs are WhatsApp users domiciled in Australia, Brazil, India, Mexico, and South Africa. (*Id*. ¶¶ 6–12.) They seek to represent a worldwide class of WhatsApp users outside the United States (and also excluding certain other countries), who between April 5, 2016, and the present sent or received any communications via WhatsApp. (*Id*. ¶ 71.) Plaintiffs allege that their end-to-end encrypted communications "have been stored by and [are] accessible to WhatsApp and Meta, notwithstanding WhatsApp's and Meta's assurances to the contrary." (*Id*. ¶ 5.) The operative complaint comprises ten claims: (1) violation of the federal Wiretap Act; (2) violation of the California Comprehensive Computer Data Access and Fraud Act ("CDAFA"); (3) violation of the California Invasion of Privacy Act ("CIPA"); (4) invasion of privacy under the California Constitution; (5) intrusion upon seclusion; (6) breach of contract; (7) breach of the implied covenant of good faith and fair dealing; (8) unjust enrichment under quasi-contract theories; (9) statutory larceny; and (10) violation of California's Unfair Competition Law ("UCL").

III. LEGAL STANDARD

A. Motion to Dismiss

To survive a Rule 12(b)(6) challenge, a plaintiff must allege "enough facts to state a claim to relief that is plausible on its face." *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim "has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The complaint must allege "more than a sheer possibility that a defendant has acted unlawfully." *Id*.

In ruling on a motion to dismiss, a court may consider only "the complaint, materials incorporated into the complaint by reference, and matters [subject to] judicial notice." *See UFCW Loc. 1500 Pension Fund v. Mayer*, 895 F.3d 695, 698 (9th Cir. 2018) (citation omitted). A court must also presume the truth of a plaintiff's allegations and draw all reasonable inferences in their favor. *See Boquist*, 32 F.4th at 773. However, a court need not accept as true "allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *See Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1008 (9th Cir. 2018) (citation omitted).

Rule 9 requires plaintiffs alleging fraud to "state with particularity the circumstances constituting fraud." Fed. R. Civ. P. 9(b). "To comply with Rule 9(b), allegations of fraud must be 'specific enough to give defendants notice of the particular misconduct which is alleged to constitute the fraud charged so that they can defend against the charge and not just deny that they have done anything wrong.'" *Bly-Magee v. California*, 236 F.3d 1014, 1019 (9th Cir. 2001) (quoting *Neubronner v. Milken,* 6 F.3d 666, 672 (9th Cir. 1993)). Accordingly, "averments of fraud must be accompanied by 'the who, what, when, where, and how' of the misconduct charged." *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003) (quoting *Cooper v. Pickett*, 137 F.3d 616, 627 (9th Cir. 1997)).

B. Motion for Sanctions

Under Rule 11, "[b]y presenting to the court a pleading, . . . an attorney . . . certifies that to the best of the person's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances: . . . the factual contentions have evidentiary support or, if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation or discovery." Fed. R. Civ. P. 11(b)(3). An attorney violates Rule 11 if (1) "the[ir] complaint is legally or factually 'baseless' from an objective perspective, and (2) if the attorney has [not] conducted 'a reasonable and competent inquiry' before signing and filing it." *Christian v. Mattel, Inc.*, 286 F.3d 1118, 1127 (9th Cir. 2002) (quoting *Buster v. Greisen,* 104 F.3d 1186, 1190 (9th Cir. 1997)). A court may impose "appropriate sanction[s]" for violations of Rule 11, but such sanctions "must be limited to what suffices to deter repetition of the conduct or comparable conduct by others similarly situated." Fed. R. Civ. P. 11(c)(1), (4).

IV. DISCUSSION

A. Motion to Dismiss

Defendants' motion to dismiss is granted. Though the entirety of the complaint is not subject to Rule 9(b) because it does not allege a "unified course of fraudulent conduct," certain claims that contain fraud as an element and the complaint's averments of fraud are subject to Rule 9(b). *Vess*, 317 F.3d at 1103–04. Those claims must be dismissed, and those averments must be disregarded, because they do not satisfy Rule 9(b)'s particularity requirement. The remainder of the claims are dismissed under Rule 12(b)(6) because, as currently pleaded, the complaint's allegations are insufficient to support a plausible inference that WhatsApp and Meta can access WhatsApp users' communications in the manner described by the complaint.

1. Applicability of Rule 9(b)

As an initial matter, the parties disagree as to whether Rule 9(b) applies to the complaint. Defendants argue that Rule 9(b) applies to the entire complaint because it alleges a "unified fraudulent course of conduct" and is therefore "grounded in fraud." (Dkt. No. 29 at 12.)[2]

[2] All references to page numbers for filings on the docket refer to ECF pagination.

Plaintiffs argue that none of their claims are subject to Rule 9(b) because none of their claims depend "entirely" on fraud. (Dkt. No. 37 at 9–11.)

Where fraud is an essential element of a claim, Rule 9(b) applies to that claim. *See Vess*, 317 F.3d at 1103–04. But even where fraud is not a necessary element of a claim, Rule 9(b) still has a role to play. In *Vess v. Ciba-Geigy Corp. USA*, the Ninth Circuit identified two such circumstances. *Id*. First, when a plaintiff "allege[s] a unified course of fraudulent conduct and rel[ies] entirely on that course of conduct as the basis of a claim," the claim is "grounded in fraud," and "the pleading of that claim as a whole must satisfy the particularity requirement of Rule 9(b)." *Id*. But in other instances, a plaintiff "may choose not to allege a unified course of fraudulent conduct in support of a claim, but rather to allege some fraudulent and some non-fraudulent conduct." *Id*. at 1104. In such cases, Rule 9(b) applies "only to 'averments' of fraud supporting a claim rather than to the claim as a whole," and "if particular averments of fraud are insufficiently pled under Rule 9(b), a district court should 'disregard' those averments, or 'strip' them from the claim. The Court should then examine the allegations that remain to determine whether they state a claim." *Id*. at 1104–05.

In *Vess*, the Ninth Circuit relied upon that distinction when analyzing the plaintiff's allegations against defendants Novartis and the American Psychiatric Association ("APA") differently. Novartis allegedly affirmatively misrepresented its relationships with the APA and other defendants and encouraged them to make misrepresentations; but Novartis also allegedly negligently failed to disclose those relationships to consumers and did not disclose important information about its drug. *Id*. at 1101, 1105–06. The Ninth Circuit observed that "at least some of Vess's non-conspiracy allegations . . . neither mention[] the word 'fraud,' nor allege[] facts that would necessarily constitute fraud." *Id*. at 1105–06. Such allegations included those regarding Novartis's negligent failure to disclose its relationships with other defendants to consumers, its failure to disclose information about its drug, and it "t[aking] steps to increase [its] sales . . . in various ways." *Id*. Accordingly, the Ninth Circuit did not apply Rule 9(b) to those allegations. *Id*. at 1106.

By contrast, the Ninth Circuit concluded that "the entirety of Vess's complaint against the APA is comprised of allegations of a unified fraudulent course of conduct" and applied Rule 9(b) to the complaint against the APA as a whole. *Id*. The complaint alleged "a fraudulent conspiracy between the APA and the other defendants," which included receiving financial contributions from Novartis, misrepresenting its connection to Novartis, lying about the reliability of diagnostic criteria for attention deficit disorder/attention deficit hyperactivity disorder, and concealing the fraud by improperly relying on testing data from tests of diagnostic criteria for unrelated medical conditions. *Id*. at 1106–07. Without the alleged fraudulent conspiracy, there would have been no claim against the APA.

Here, the complaint does not allege a unified fraudulent course of conduct such that the entire complaint is subject to Rule 9(b). To be sure, the complaint alleges that Defendants misrepresented that WhatsApp communications were end-to-end encrypted and that they could not access users' communications, in addition to taking steps to prevent the dissemination of the truth including "siloing workers" and "imposing onerous nondisclosure agreements." (*E.g.*, Compl. ¶¶ 1–3, 38–39, 70.) But the complaint also alleges that Defendants acted wrongfully simply by storing and accessing users' communications even if they had been silent as to whether they could access users' communications or had made the alleged misstatements without fraudulent intent. (*E.g.*, *id*. ¶¶ 36–37, 83, 117.) The allegations in the latter category, though related to those in the former category, do not allege facts "that would necessarily constitute fraud." Plaintiffs' allegations against Defendants therefore do not rely entirely on a unified fraudulent course of conduct. Accordingly, while the entire complaint is not subject to Rule 9(b), the allegations constituting averments of fraud are subject to Rule 9(b).

The allegations that Defendants intentionally misrepresented that WhatsApp users' communications were end-to-end encrypted and that Defendants could not access the communications are subject to Rule 9(b) and fail to meet Rule 9(b)'s particularity requirement. Specifically, the complaint alleges that Meta's "[s]enior leadership" tried to hide the truth; that Defendants have been "willfully misrepresenting" that WhatsApp messages are private and

inaccessible even to WhatsApp and Meta; that Meta showed a "brazen willingness to mislead WhatsApp users regarding its and WhatsApp's ability to access users' encrypted communications"; that Meta "kept the circle of fraud small" and "tried to prevent the truth from coming out"; that Meta is "willing to lie to achieve its priorities"; that Meta "fraudulently appropriated" Plaintiffs' personal information; and that Meta engaged in an "intentional intrusion" into private messages while being "well aware" that its promises of privacy were "false." (*E.g.*, Compl. ¶¶ 2, 5, 39, 70, 133, 144, 178.) These allegations lack the requisite "'who, what, when, where, and how' of the misconduct charged." *Vess*, 317 F.3d at 1106 (quoting *Cooper*, 137 F.3d at 627). They do not say which "senior leadership" engaged in this fraud, what facts show when the decisions to engage in this fraud occurred, or how senior leadership knew the messages could in fact be accessed. The complaint also alleges that Defendants took various steps to prevent the dissemination of the truth regarding their ability to access user messages, including siloing workers, telling them to "stay in [their] lane," and imposing nondisclosure agreements. (*Id*. ¶¶ 2, 39.) These allegations likewise fail to meet Rule 9(b) because they lack details such as who made those statements and when those statements were made and those actions were taken. Accordingly, these allegations are disregarded for purposes of assessing the motion to dismiss.

However, most of the complaint's allegations regarding Defendants' ability to access users' messages and the statements that Defendants made in WhatsApp's Privacy Policy or on WhatsApp's website are not subject to Rule 9(b). As described above, those allegations do not involve facts that would necessarily constitute fraud and thus do not constitute averments of fraud. *See Vess*, 317 F.3d at 1105–06. These allegations are retained for consideration for purposes of deciding the motion to dismiss.

2. Wiretap Act Claim

The Wiretap Act prohibits the intentional interception of the contents of any wire, oral, or electronic communication through the use of a device without consent. *See* 18 U.S.C. §§ 2510, 2511. Plaintiffs' Wiretap Act claim is not subject to dismissal under Rule 9(b) because it does

not rely on Plaintiffs' allegations that Defendants knowingly misrepresented the privacy of WhatsApp communications. Even if Defendants had been silent as to the privacy of WhatsApp messages, a claim could still be stated based on an alleged interception without obtaining users' consent to access the messages.

However, the complaint fails to state a Wiretap Act claim because it does not plausibly allege that Defendants can, in fact, access users' encrypted WhatsApp communications. The complaint contains no details about the factual basis for its allegations that Defendants' employees can access users' messages by sending a "task" and receiving a "widget" in response. It is insufficient for purposes of Rule 8 to merely state the conclusion that Defendants' employees can access users' messages in this manner and can do so "without any scrutiny." (Compl. ¶ 36.) Rather, the complaint must provide factual allegations as to the plausible basis for that conclusion.

Here, the only factual allegation on that front is Plaintiffs' assertion that "whistleblowers here have explained" as much. (*Id*.) But where there are essentially no other non-conclusory factual allegations providing a basis for Plaintiffs' assertions regarding Defendants' ability to access users' messages, the complaint needs to describe some basic facts about how each whistleblower knows about what they have described, and if the knowledge is not firsthand, why it is otherwise plausibly inferred to be reliable. To be clear, the Court is not endorsing Defendants' proposal to impose a Private Securities Litigation Reform Act standard generally to factual allegations sourced from whistleblowers (*see* Dkt. No. 29 at 15), nor is the Court requiring that Plaintiffs identify their whistleblower(s) in an amended complaint. Instead, merely stating that the complaint's allegations came from whistleblowers without further elaboration is insufficient on its own to make it plausible that WhatsApp employees have been accessing its user messages in the manner alleged by the whistleblowers.

Also, even assuming that the whistleblower allegations have a sufficient factual basis to support a plausible inference that Defendants can access WhatsApp users' messages, those allegations on their own do not support a plausible inference that Defendants accessed users'

messages for purposes other than operating the WhatsApp service or Meta's business, as authorized under the Wiretap Act. The complaint alleges that "[a] worker need only send a 'task' . . . to a Meta engineer with an explanation that they need access to WhatsApp messages for their job." (Compl. ¶ 36.) Without more, that allegation does not contain enough information to support an inference that Defendants were accessing users' messages for purposes beyond those necessarily incident to operating WhatsApp or to the protection of Meta's rights or property. *See* 18 U.S.C. § 2511(2)(a)(i) ("It shall not be unlawful under this chapter for . . . an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service.").

Accordingly, Plaintiffs' Wiretap Act claim is dismissed. Meta also argues that this claim should be dismissed because it seeks to apply the Wiretap Act extraterritorially to conduct that occurred outside of the United States. (*See* Dkt. No. 29 at 20.) However, the complaint alleges that Defendants accessed users' messages in the United States, which is where Defendants' servers and systems are located. (Compl. ¶¶ 90, 104, 114.) That is sufficient to support a plausible inference that Defendants' interception of users' WhatsApp messages occurred in the United States. *See United States v. Luong*, 471 F.3d 1107, 1109 (9th Cir. 2006) ("[A]n interception occurs where the tapped phone is located *and* where law enforcement officers first overhear the call."). The Court therefore declines to dismiss the Wiretap Act claim on this basis.

3. CDAFA Claim

Plaintiffs bring claims under several provisions of CDAFA. Once such provision, section 502(c)(1), applies to anyone who "[k]nowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data." Cal. Penal Code § 502(c)(1). At

oral argument, Plaintiffs conceded the section 502(c)(1) claim contains fraud as an element. The claim is therefore subject to dismissal under Rule 9(b) and fails to satisfy Rule 9(b)'s particularity requirement for the reasons described above.

As to Plaintiffs' remaining CDAFA claims, disregarding the complaints' allegations regarding Defendants' intentional misrepresentations under Rule 9(b) is not fatal, as those claims require only that Defendants have accessed users' messages "knowingly and without permission." *See id*. § 502(c)(2), (6)–(8), (12). Thus, even if Defendants had never made any statements at all regarding the secrecy or privacy of WhatsApp messages, a CDAFA claim could theoretically be stated if the employees who were accessing the messages knew that Meta had not obtained users' permission for such access. However, for the reasons discussed as to the Wiretap Act claim, the complaint fails to plausibly allege that Defendants accessed users' messages at all under Rule 8. Accordingly, the motion to dismiss this claim is granted.

Defendants argue that the CDAFA claim should be dismissed for two additional reasons. First, they argue that the claim attempts to apply CDAFA extraterritorially. However, as discussed above, the complaint plausibly alleges that Defendants accessed users' messages in California, where their servers and systems are located. Therefore, Plaintiffs' CDAFA claim does not arise from conduct that occurred outside of California, even if Plaintiffs themselves are located outside of California. *See Lineberry v. AddShopper, Inc.*, No. 23-cv-01996-VC, 2025 WL 551864, at *3 (N.D. Cal. Feb. 19, 2025) (dismissing CDAFA claim because of the absence of allegations of wrongful conduct that occurred in California).

Second, Defendants argue that the complaint fails to plausibly allege that Plaintiffs suffered a cognizable harm under CDAFA. (*See* Dkt. No. 29 at 19.) The complaint contains only conclusory allegations that Defendants' accessing of WhatsApp users' messages "caused loss to Plaintiffs and Class Members" and that Defendants have been "unjustly enriched." (Compl. ¶ 105.) Absent from the complaint is any explanation of what loss Plaintiffs experienced and what benefit Defendants allegedly received. *See Smith v. Rack Room Shoes,*

Inc., No. 24-cv-06709-RFL, 2025 WL 2210002, at *3 (N.D. Cal. Aug. 4, 2025). The CDAFA claim is therefore dismissed on this additional basis as well.

4. CIPA Claim

CIPA prohibits the intentional interception of a communication without the consent of all parties to the communication. Cal. Penal Code §§ 631(a), 632(a). For the same reasons discussed as to the Wiretap Act claim, this claim is not subject to dismissal under Rule 9(b) because it does not require fraud as an element, nor does it rely on the disregarded allegations regarding Defendants' intentional misrepresentations. However, the motion to dismiss this claim is granted because the complaint fails to plausibly allege under Rule 8 that Defendants accessed, and therefore intercepted, users' communications and that Defendants did so for reasons besides operating WhatsApp. Defendants also argue that this claim should be dismissed because it seeks to apply CIPA extraterritorially. (Dkt. No. 29 at 20.) As discussed above, the complaint plausibly alleges that the conduct at issue in this case, the accessing of WhatsApp users' messages, occurred in California. *See Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1079 (N.D. Cal. 2023). The Court therefore declines to dismiss the complaint on this basis.

5. Invasion of Privacy and Intrusion Upon Seclusion Claim

To plead an invasion of privacy claim, a plaintiff must allege (1) a legally protected privacy interest, (2) a reasonable expectation of privacy under the circumstances, and (3) conduct that amounts to a "serious, egregious invasion of the protected privacy interest." *In re Google, Inc. Privacy Pol'y Litig.*, 58 F. Supp. 3d 968, 985 (N.D. Cal. 2014). A claim for intrusion upon seclusion requires that a plaintiff allege (1) that the defendant intentionally intruded into a "place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy"; and (2) that the intrusion occurred "in a manner highly offensive to a reasonable person." *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (2009).

The complaint fails to state invasion of privacy and intrusion upon seclusion claims under Rule 9(b). Without Plaintiffs' allegations regarding Defendants' intentional misrepresentations and attempts to prevent dissemination of the truth, the complaint fails to plausibly allege that

Defendants' accessing of users' messages was "highly offensive" or a "serious, egregious" invasion of privacy. The complaint's remaining allegations do not support a plausible inference that Defendants' access of users' messages was for an improper purpose. To the contrary, the complaint's allegations suggest that Defendants' accessing of users' messages was incident to their operation of WhatsApp—*i.e.*, "routine behavior" rather than "secret or deceptive data collection" capable of giving rise to a privacy violation. *Hubbard v. Google LLC*, No. 19-cv-07016-SVK, 2024 WL 3302066, at *7 (N.D. Cal. July 1, 2024). Furthermore, the complaint fails to plausibly allege that Defendants intruded on WhatsApp users' privacy because it does not plausibly allege that Defendants accessed users' WhatsApp messages under Rule 8, as discussed above. Accordingly, the motion to dismiss these claims is granted.

Defendants also argue that the invasion of privacy claim must be dismissed because Plaintiffs have "no connection to California." (Dkt. No. 29 at 19.) However, Plaintiffs "have plausibly alleged that the conduct causing them harm occurred and emanated from California," which is "sufficient at this juncture." *Doe*, 690 F. Supp. 3d at 1080–81.

6. Breach of Contract Claim

The complaint fails to state a breach of contract claim. This claim is not subject to dismissal under Rule 9(b), and disregarding the complaint's allegations about Defendants' intentional misrepresentations is not fatal to the claim, as it is immaterial whether the promises providing the basis for Plaintiffs' breach of contract claim were intentional misrepresentations. *Cf. Roth v. Malson*, 67 Cal. App. 4th 552, 557 (1998) ("Contract formation is governed by objective manifestations, not subjective intent of any individual involved."). However, the complaint fails to plausibly allege under Rule 8 that Defendants breached their promises regarding the privacy of WhatsApp messages, as the complaint's allegations do not support a plausible inference that Defendants can access users' WhatsApp messages in the manner that the complaint asserts. *See Oasis W. Realty, LLC v. Goldman*, 51 Cal. 4th 811, 821 (2011). Therefore, the motion to dismiss this claim is granted.

7. Breach of Implied Covenant Claim

For the same reasons that the complaint fails to state a breach of contract claim, it also fails to state a breach of implied covenant claim. Although this claim is not subject to dismissal under Rule 9(b) and disregarding the complaint's averments of fraud is not outcome determinative, the complaint fails to plausibly allege that Defendants can access WhatsApp users' messages under Rule 8.

8. Unjust Enrichment Claim

The complaint fails to state an unjust enrichment claim. "A claim for unjust enrichment is essentially a claim for restitution, the elements of which are that the defendant received and unjustly retained a benefit at the plaintiff's expense." *See Lau v. Gen Digital Inc.*, No. 22-cv-08981-RFL, 2024 WL 1880161, at *5 (N.D. Cal. Apr. 3, 2024) (citing *Durell v. Sharp Healthcare*, 183 Cal. App. 4th 1350, 1370 (2010)), *aff'd sub nom. Karwowski v. Gen Digital, Inc.*, No. 24-7213, 2025 WL 3002610 (9th Cir. Oct. 27, 2025). Because the complaint fails to plausibly allege under Rule 8 that Defendants acted wrongfully by accessing WhatsApp users' communications, the motion to dismiss this claim is granted. The claim is also dismissed because Plaintiffs fail to plausibly allege that Defendants received and unjustly retained a benefit at their expense. The complaint contains only conclusory allegations that "[a]s a result of Defendants' tortious acts, Defendants received and unjustly retained a benefit at the expense of Plaintiffs, Class Members, and other WhatsApp users," and that "[i]t would be unjust for Defendants to retain the value of Plaintiffs' property and any profits earned thereon." (Compl. ¶¶ 169–70.) That is insufficient to support a plausible inference that Defendants received and unjustly retained a benefit as a result of their alleged accessing of WhatsApp users' messages. *See Rojas v. Bosch Solar Energy Corp.*, 386 F. Supp. 3d 1116, 1131 (N.D. Cal. 2019). The unjust enrichment claim is therefore dismissed with leave to amend so Plaintiffs can correct this deficiency.

9. Statutory Larceny Claim

The complaint fails to state a claim for statutory larceny. California Penal Code section 496(a) prohibits receiving property "that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained." Cal Pen. Code § 496(a). Section 484(a) defines "theft," explaining:

> Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall *fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property*, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

Id. § 484(a) (emphasis added). Because this claim requires proof of fraudulent conduct, which Plaintiffs conceded at oral argument, it is subject to dismissal under Rule 9(b). Without the complaint's allegations (a) that Defendants intentionally and deceptively designed the process by which they access WhatsApp users' messages and (b) that they were able to do so because of their intentional misrepresentations regarding WhatsApp's privacy, the complaint fails to plausibly allege that Defendants obtained users' messages in a manner constituting theft. Accordingly, the motion to dismiss this claim is granted.

Defendants raise two additional arguments that they claim support dismissal of this claim. First, Defendants argue that this claim seeks to apply the California civil theft statute extraterritorially. But as discussed above, Defendants' servers and systems are in California, and Defendants allegedly accessed WhatsApp users' messages from California. The Court therefore declines to dismiss the statutory larceny claim on this basis. Second, Defendants argue that the complaint fails to plausibly allege that Plaintiffs suffered "actual damages." (Dkt. No. 29 at 18.) The complaint alleges only (a) that WhatsApp users' messages were appropriated without their consent and (b) that Defendants obtained users' messages for "commercial purposes and . . . financial benefit." (Compl. ¶¶ 178–79.) But mere misappropriation of users' messages is insufficient to support a plausible inference of actual damages, and the complaint does not

specify what financial benefit Defendants allegedly received or explain how Defendants' receipt of that benefit caused Plaintiffs actual damages. *See Tanner v. Acushnet Co.*, No. 23-cv-00346-HDV, 2023 WL 8152104, at *10 (C.D. Cal. Nov. 20, 2023); *see also Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1042 (N.D. Cal. 2018). The statutory larceny claim is therefore dismissed for this additional reason.

10. UCL Claim

Neither the unlawful nor the unfair prong of the UCL requires fraud as an element or relies on the disregarded allegations regarding intentional misrepresentations, so the UCL claim is not subject to dismissal under Rule 9(b). However, the claim fails to state a plausible claim under Rule 8, for the reasons explained above. Because the complaint fails to state a claim for any unlawful conduct, it too fails to state an unlawful prong claim. Moreover, after disregarding the allegations described above as to the statutory larceny claim, the complaint fails to state an unfair prong claim because it does not plausibly allege that Defendants improperly accessed users' messages. Accordingly, the motion to dismiss the UCL claim is granted.

Defendants argue that dismissal of this claim is warranted for two additional reasons. First, Defendants argue that this claim seeks to apply the UCL extraterritorially. As discussed above, Plaintiffs' other statutory and constitutional claims do not entail applying the relevant provisions extraterritorially. The alleged unlawful/unfair conduct occurred in California. Applying the UCL to that conduct does not entail applying the UCL extraterritorially. *See Hughes v. Apple, Inc.*, No. 22-cv-07668-VC, 2024 WL 4828072, at *3 (N.D. Cal. Nov. 18, 2024).

Second, Defendants contend that that the complaint fails to plausibly allege that Plaintiffs suffered a cognizable harm under the UCL. The complaint alleges that Plaintiffs and other WhatsApp users suffered a diminution in value of their WhatsApp messages, lost the "benefit of their bargain with Defendants," and experienced "damage[s] to and loss of" their "property right[s] to control the dissemination and use of their personal information and communications." (Compl. ¶¶ 188–89.) But Plaintiffs have not plausibly alleged that there exists a market for their

WhatsApp messages, that they or members of the putative class intend to participate in such a market, or that they paid money or gave something else of value to Defendants to use WhatsApp. *See Doe*, 690 F. Supp. 3d at 1089–91. Plaintiffs' UCL claim is therefore dismissed for this additional reason.

11. Shotgun Pleading

Defendants also seek to dismiss the complaint on the basis that it is a "shotgun pleading." Dismissal is not granted on this basis. The complaint is not a shotgun pleading. Even if (a) each of Plaintiffs' counts adopts the allegations of the preceding counts and (b) some of the counts assert multiple claims for relief, the complaint's allegations are not so indecipherable so as to violate Rule 8. *See In re Meta Pixel Tax Filing Cases*, 724 F. Supp. 3d 987, 1005 (N.D. Cal. 2024).

B. Motion for Sanctions

The motion for sanctions is denied. Defendants argue (a) that the complaint is factually baseless, suggesting that Plaintiffs filed the complaint without conducting a reasonable pre-complaint investigation, and (b) that Plaintiffs maintained the complaint in the face of contrary evidence proving that their claims were false. (Dkt. No. 38 at 15–19.) Defendants proffer evidence that they cannot access messages that are encrypted in transit or stored in encrypted form. But the gravamen of the complaint is that Defendants can access users' WhatsApp messages, including in real-time as they are sent, despite publicly stating that they cannot. Breaking end-to-end encryption is not the only means by which that could happen. As the expert declaration submitted by Plaintiffs confirms, Defendants' evidence does not conclusively preclude the possibility that the whistleblowers' allegations are true and thus does not provide a basis for Rule 11 sanctions. (*See* Dkt. No. 40-5 at ¶¶ 7–14.)

V. CONCLUSION

For the foregoing reasons, the motion to dismiss is granted and the motion for sanctions is denied. Dismissal is with leave to amend because it appears that Plaintiffs could potentially cure the deficiencies identified with more detailed pleading. If Plaintiffs wish to file an amended

complaint correcting the deficiencies identified above, counsel shall do so by **August 13, 2026**. The amended complaint may not add new claims or parties, or otherwise change the allegations except to correct the identified deficiencies, absent leave of the Court or stipulation by the parties pursuant to Federal Rule of Civil Procedure 15. If no amended complaint is filed by that date, the complaint will remain dismissed with prejudice, judgment will be entered in favor of Defendants, and the case will be closed.

IT IS SO ORDERED.

Dated: July 23, 2026

RITA F. LIN
United States District Judge