UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MATTHEW CAMPBELL, et al.,

Plaintiffs,

v.

FACEBOOK INC.,

Defendant.
_____/

No. C 13-5996 PJH

ORDER GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS

Defendant's motion to dismiss plaintiffs' consolidated amended complaint came on for hearing before this court on October 1, 2014. Plaintiffs Matthew Campbell, Michael Hurley, and David Shadpour ("plaintiffs") appeared through their counsel, Michael Sobol. Defendant Facebook, Inc. ("defendant" or "Facebook") appeared through its counsel, Joshua Jessen. Having read the parties' papers and carefully considered their arguments and the relevant legal authority, and good cause appearing, the court hereby GRANTS in part and DENIES in part defendant's motion as follows.

BACKGROUND

This is a privacy case involving the scanning of messages sent on Facebook's social media website. Facebook describes itself as the "world's largest social networking platform," with approximately 1.2 billion users worldwide. Facebook users are able to share content – such as photos, text, and video – with other users. Users can select the group of people with whom they wish to share this content, and may choose to share certain information publicly (i.e., with all Facebook users), or may choose to share certain information only with their "friends" (i.e., Facebook users with whom they have mutually agreed to share content). Facebook users may also choose to share certain information

privately, with just one other Facebook user, through the use of a "private message." While not identical to email, a private message is analogous to email, in that it involves an electronic message sent from one user to one or more other users. Facebook users can access a "messages" inbox through the Facebook website, which is akin to an email inbox. This suit arises out of Facebook's handling of these "private messages."

Plaintiffs allege that Facebook scans the content of these private messages for use in connection with its "social plugin" functionality. Specifically, certain websites have a Facebook "like" counter displayed on their web pages, which enables visitors of the page to see how many Facebook users have either clicked a button indicating that they "like" the page, or have shared the page on Facebook. In essence, the "like" counter is a measure of the popularity of a web page.

Plaintiffs allege that Facebook scans the content of their private messages, and if there is a link to a web page contained in that message, Facebook treats it as a "like" of the page, and increases the page's "like" counter by one. Plaintiffs further allege that Facebook uses this data regarding "likes" to compile user profiles, which it then uses to deliver targeted advertising to its users. Plaintiffs allege that the messaging function is designed to allow users to communicate privately with other users, and that Facebook's practice of scanning the content of these messages violates the federal Electronic Communications Privacy Act ("ECPA," also referred to as the "Wiretap Act"), as well as California's Invasion of Privacy Act ("CIPA"), and section 17200 of California's Business and Professions Code.

Plaintiffs seek to represent a nationwide class of "all natural person Facebook users located within the United States who have sent or received private messages that included URLs in their content, from within two years before the filing of this action up through and including the date when Facebook ceased its practice." Consolidated Amended Complaint ("CAC"), ¶ 59.

DISCUSSION

A. Legal Standard

A motion to dismiss under Rule 12(b)(6) tests for the legal sufficiency of the claims alleged in the complaint. Ileto v. Glock, Inc., 349 F.3d 1191, 1199-1200 (9th Cir. 2003). Review is limited to the contents of the complaint. Allarcom Pay Television, Ltd. v. Gen. Instrument Corp., 69 F.3d 381, 385 (9th Cir. 1995). To survive a motion to dismiss for failure to state a claim, a complaint generally must satisfy only the minimal notice pleading requirements of Federal Rule of Civil Procedure 8.

Rule 8(a)(2) requires only that the complaint include a "short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). Specific facts are unnecessary – the statement need only give the defendant "fair notice of the claim and the grounds upon which it rests. Erickson v. Pardus, 551 U.S. 89, 93 (citing Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 555 (2007)). All allegations of material fact are taken as true. Id. at 94. However, a plaintiff's obligation to provide the grounds of his entitlement to relief "requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." Twombly, 550 U.S. at 555 (citations and quotations omitted). Rather, the allegations in the complaint "must be enough to raise a right to relief above the speculative level. Id.

A motion to dismiss should be granted if the complaint does not proffer enough facts to state a claim for relief that is plausible on its face. See id. at 558-59. "[W]here the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged – but it has not show[n] – that the pleader is entitled to relief. Ashcroft v. Iqbal, 556 U.S. 662, 679 (2009).

In addition, when resolving a motion to dismiss for failure to state a claim, the court may not generally consider materials outside the pleadings. Lee v. City of Los Angeles, 250 F.3d 668, 688 (9th Cir. 2001). There are several exceptions to this rule. The court may consider a matter that is properly the subject of judicial notice, such as matters of public record. Id. at 689; see also Mack v. South Bay Beer Distributors, Inc., 798 F.2d

1279, 1282 (9th Cir. 1986) (on a motion to dismiss, a court may properly look beyond the complaint to matters of public record and doing so does not convert a Rule 12(b)(6) motion to one for summary judgment). Additionally, the court may consider exhibits attached to the complaint, see Hal Roach Studios, Inc. v. Richard Feiner & Co., Inc., 896 F.2d 1542, 1555 n.19 (9th Cir. 1989), and documents referenced by the complaint and accepted by all parties as authentic. See Van Buskirk v. Cable News Network, Inc., 284 F.3d 977, 980 (9th Cir. 2002).

B. Legal Analysis

1. Wiretap Act

The Wiretap Act provides for civil penalties against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). As the statutory text indicates, the focus of this provision is on the interception of the communication itself. While another provision of the Wiretap Act prohibits the use of the contents of a communication, that prohibition applies only if the interception itself is unlawful under section 2511(1)(a). Specifically, section 2511(1)(d) applies to any person who "intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication," but only if that person knows or has reason to know "that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection." See 18 U.S.C. § 2511(1)(d) (emphasis added). In other words, if there is no unlawful interception, there can be no unlawful use.

Facebook argues that this distinction between "interception" and "use" favors dismissal of plaintiffs' Wiretap Act claim. According to Facebook, plaintiffs' real objection is not to Facebook's interception of private messages, but rather, to Facebook's use of the information. Facebook argues that it must have access to the messages in order to facilitate their delivery, so there cannot be any unlawful interception; and thus, there can be no unlawful use. See Noel v. Hall, 568 F.3d 743, 751 (9th Cir. 2009) ("use" provision "protects against the dissemination of private communications that have been unlawfully

intercepted.") (emphasis in original).

However, the Noel court also made clear that the term "interception" should not be interpreted as narrowly as urged by Facebook. The Noel court quoted the Wiretap Act's definition of "intercept," which is "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device," and then held that an "acquisition" occurs "when the contents of a wire communication are captured or redirected in any way." Noel, 568 F.3d at 749 (emphasis added).

At this stage of the case, the court is unable to determine whether Facebook unlawfully "redirected" the content of plaintiffs' private messages. While Facebook must certainly receive the contents of any message in order to transmit it to the recipient(s), there is no evidentiary record from which the court can determine whether Facebook "redirected" messages in order to scan their content for use in increasing "like" counters and for targeted advertising.

In the CAC, plaintiffs allege that Facebook uses a software application called a "web crawler" to scan any URLs that are contained in messages and to send server requests to that web page. CAC, ¶ 25. If true, the use of this "web crawler" could constitute a "redirection" of the contents of users' messages, and therefore, a separate "interception" under the Wiretap Act. Because the court takes the complaint's allegations as true, it would be premature to find that plaintiffs' claims center only around Facebook's use, not its interception, of users' private messages.

Facebook raises a second threshold challenge to plaintiffs' Wiretap Act claim. It argues that any actionable "interception" under the Wiretap Act must involve the communication being acquired during transmission, rather than during storage. Facebook points out that Congress created a separate statute, the Stored Communications Act, to address access to stored electronic communications. Facebook argues that the "sequence of actions that plaintiffs allege involves use of content already in storage." Dkt. 29 at 27.

However, the CAC does indeed allege that "Facebook's interception occurred in

transit, in transmission, and/or during transfer of users' private messages." CAC, ¶ 25. While Facebook may ultimately produce evidence showing that the messages were actually accessed while in storage, not during transmission, that issue is premature at this stage of the case, and would be better addressed as part of a motion for summary judgment with a more developed factual record. See also In re Yahoo Mail Litigation, 7 F.Supp.3d 1016, 1027-28 (N.D. Cal. 2014).

Having addressed the threshold issues regarding plaintiffs' Wiretap Act claim, the court now turns to Facebook's primary arguments: that any alleged interception falls within the "ordinary course of business" exception to the Wiretap Act, and that plaintiffs consented to any alleged interception of their messages.

a. "Ordinary course of business" exception

As mentioned above, the Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). The statute then further defines "electronic, mechanical, or other device" as "any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than" a device or apparatus that is "being used by a provider of wire or electronic communication service in the ordinary course of its business." 18 U.S.C. § 2510(5). Essentially, the Wiretap Act creates an exception for interceptions conducted by an electronic communications service provider occurring in "the ordinary course of its business."

The scope of this "ordinary course of business" exception has been the subject of extensive litigation in this district. The parties focus on two cases in particular: In re Google Inc. Gmail Litigation, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013) (referred to as "Gmail") and In re Google Inc. Privacy Policy Litigation, 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013) (referred to as "Google").

The Gmail case involved allegations that the defendant, Google Inc., was scanning the content of users' emails in order to facilitate its delivery of targeted advertising, and to create "user profiles to serve their profit interests that were unrelated to providing email

services to particular users." Plaintiffs asserted that the email scanning violated the Wiretap Act, and Google moved to dismiss based on the "ordinary course of business" exception. The court denied the motion to dismiss, finding that the "ordinary course of business" exception must be given a "narrow reading" that requires "some nexus between the need to engage in the alleged interception and the subscriber's ultimate business, that is, the ability to provide the underlying service or good." Gmail at *11. In other words, the court held that the interception must "facilitate[]" or be "incidental" to the provision of the electronic communication service at issue. Id. Plaintiffs alleged that Google had intercepted emails "for the purposes of creating user profiles and delivering targeted advertising, which are not instrumental to Google's ability to transmit emails." Id. Plaintiffs also alleged that the interceptions of emails for targeting ads and creating user profiles occurred separately from other processes that were related to the transmission of emails, such as spam filtering, antivirus protection, and spell check. Thus, the complained-about interceptions were "physically and purposively unrelated to Google's provision of email services." Id. Additionally, the Gmail court further found that the defendant's actions were in violation of its own internal policies, and thus could not be considered within the ordinary course of its business.

While the Google case involved the same defendant as the Gmail case, it involved a different Google product, and thus, a different application of the "ordinary course of business" exception. Rather than involving claims of scanning users' emails, Google involved allegations that Google would combine personal information collected from its different services – Google search, Gmail, YouTube, Google Maps, Picasa, etc. – in order to create a single user profile. The plaintiffs pointed out that Google previously allowed its users to keep information gathered from one Google product separate from information gathered from other Google products, but then changed its policy to commingle all of that data. Plaintiffs alleged that this commingling violated the Wiretap Act, and Google moved to dismiss, invoking the "ordinary course of business" exception.

The Google court rejected a "narrow read" of the exception that would be "limited to

only action taken to deliver the electronic communication." Google at *10. Instead, the court found that "Congress specifically chose the broader term 'business' that covers more far-ranging activity." Id. The pairing of the term "business" with the terms "ordinary course" further "suggest[ed] an interest in protecting a provider's customary and routine business practices." Id. The Google court found that targeted advertising was indeed within Google's ordinary course of business, and dismissed plaintiffs' Wiretap Act claim.

The Ninth Circuit has not yet ruled on the scope of the "ordinary course of business" exception. In the absence of any such authority, both the Gmail court and the Google court looked to cases from other circuit courts, and gave careful consideration to the Second Circuit's decision in Hall v. Earthlink Network, Inc., 396 F.3d 500 (2nd Cir. 2005), and the Tenth Circuit's decision in Kirch v. Embarq Management Co., 702 F.3d 1245 (10th Cir. 2012).

In Hall, an email user had a dispute with his email provider (Earthlink) that resulted in the termination of his email account. However, even after the termination, Earthlink continued to receive emails that were sent to the user's address, and the user complained that the receipt of his messages constituted an unlawful "interception" under the Wiretap Act. The court found that receiving the emails was within Earthlink's ordinary course of business, and noted that, at the relevant time, Earthlink did not have the technological capacity to "bounce back" emails that were sent to a terminated email address.

In Kirch, the plaintiffs' internet service provider (Embarq) placed a device on its servers that redirected its users' Internet traffic to a third-party company (NebuAd) that tracked which websites the users visited and used that information to target ads. The district court granted summary judgment on two bases – but not on the ordinary course of business exception. Instead, the district court first found that Embarq did not actually intercept the data, and instead merely siphoned it off to NebuAd. Second, the district court found that plaintiffs had consented to the interception by agreeing to Embarq's privacy policy. On appeal, the Tenth Circuit seemingly agreed with the first of the district court's reasons, but also applied the ordinary course of business exception, finding that Embarq

had no more access to the users' data than it did in the ordinary course of its business. And because there was no aiding-and-abetting liability under the Wiretap Act, Embarq could not be held responsible for any alleged interception by NebuAd.

While Hall and Kirch present useful discussions of the "ordinary course of business" exceptions, the court ultimately finds that the factual differences preclude any meaningful application of those courts' reasoning to this case. In Hall, there was no "interception" analogous to the alleged interception in this case – instead, the complained-about conduct was nothing more than the receipt of emails itself, which would be "ordinary" even under the narrowest view of the word. And while Kirch involved analysis of users' web activity to aid in targeting advertising (similar to the allegations in the present case), the court's dismissal of the Wiretap Act claim was based primarily on the fact that any unlawful interception was performed by a third-party, rather than by the defendant. Notably, the Kirch court did not explain whether its decision would have been the same if the defendant itself had analyzed the web traffic to deliver targeted advertising, and the court never expressly held that targeted-ad-analysis was within the ordinary course of Embarq's business as an internet service provider. Instead, the court held only that Embarq was not involved in any such analysis, and thus, had the same level of access that it would have even in the absence of NebuAd's analysis. Because there are no such third-party issues in this case, the court finds that Kirch is not applicable.

Instead, the court finds the analyses of the Gmail and Google courts to provide the most value to the present case. To summarize the difference between the two rulings, Gmail took a narrow view of the "ordinary course of business" exception and held that it covers only interceptions that are "instrumental" (or "facilitate[]" or are "incidental") to the provision of electronic communication services, while Google took the broader view that the interception need only be part of a defendant's "customary and routine" business practices. In so doing, both courts presented persuasive reasons to avoid an overly broad or narrow approach.

For instance, the Google court rejected a "narrow read" of the exception that would

be "limited to only action taken to deliver the electronic communication." Instead, as mentioned above, the Google court found that "Congress specifically chose the broader term 'business' that covers more far-ranging activity." Google at *10. The Google court rejected the plaintiffs' argument that the exception should cover only "necessary" activities, pointing out that such a rule would "beg[] the question of what exactly it means for a given action to be 'necessary' to the delivery of Gmail." Google at *11.

While the Google court emphasized the need to give meaning to the term "business," the Gmail court cautioned that an overly broad interpretation of the exception would read the word "ordinary" out of the statute. Gmail at *8 ("The presence of the modifier 'ordinary' must mean that not everything Google does in the course of its business would fall within the exception."). The Gmail court ultimately found that the exception must be given a "narrow reading" that requires "some nexus between the need to engage in the alleged interception and the subscriber's ultimate business, that is, the ability to provide the underlying service or good." Gmail at *11.

The court agrees that the word "ordinary" serves to narrow the exception, while the term "business" serves to broaden it. The court also finds it significant that the statute exempts activities conducted by a "provider of wire or electronic communication service in the ordinary course of its business." The use of the word "its" indicates that the court must consider the details of Facebook's business, and must not rely on a generic, one-size-fits-all approach that would apply the exception uniformly across all electronic communication service providers. However, Facebook has not offered a sufficient explanation of how the challenged practice falls within the ordinary course of its business, which prevents the court from determining whether the exception applies.

For instance, in both its motion and its reply, Facebook emphasizes that plaintiffs' original complaint accused Facebook of using users' message content to target advertising, but points out that plaintiffs "have now abandoned their inaccurate, advertising-related allegations (except for some lingering amorphous allegations)." Dkt. 29 at 8. Facebook repeatedly characterizes plaintiffs' advertising-related allegations as "false claims," or

"factually incorrect," or lacking "any factual basis whatsoever." Dkt. 29 at 14, 22; Dkt. 35 at 8. However, Facebook then turns around and argues that serving targeted advertisements is indeed the type of "legitimate purpose" that warrants application of the "ordinary course of business" exception, and that "systematic conduct of the type alleged by plaintiffs that generates revenue for a company is the very essence of a company acting in the ordinary course of business." Dkt. 29 at 22.

The court finds it problematic that Facebook is attempting to have it both ways by maintaining that plaintiffs' advertising-related allegations lack any factual basis, and even to emphasize that the allegations have been removed apart from a "few conclusory stragglers," but then using those largely-removed allegations to invoke the "ordinary course of business" exception. Regardless, if the court does take as true plaintiffs' remaining allegations regarding targeted advertising, it still finds an insufficient record on which to base a finding that the challenged practice is within the ordinary course of Facebook's business. Facebook's unwillingness to offer any details regarding its targeted advertising practice prevents the court from being able to determine whether the specific practice challenged in this case should be considered "ordinary."

The court rejects the suggestion that any activity that generates revenue for a company should be considered within the "ordinary course of its business." At the hearing, Facebook's counsel suggested that, because the practice is in the service of making money, it must necessarily fall within the ordinary course of business. However, as discussed above, the statute's inclusion of the word "ordinary" implies some limits on a company's ability to self-define the scope of the exception. An electronic communications service provider cannot simply adopt any revenue-generating practice and deem it "ordinary" by its own subjective standard. The court instead finds that any interception falling within the exception must be related or connected to an electronic communication provider's service, even if it does not actually facilitate the service. While the court agrees with the Google court's holding that the exception must cover more than just "necessary" activities, it also agrees with the Gmail court's finding that there must be "some nexus

between the need to engage in the alleged interception and the subscriber's ultimate business, that is, the ability to provide the underlying service or good." Based on the current record, the court cannot find any facts alleged in the complaint or facts presented by Facebook that indicate a nexus between Facebook's alleged scanning of users' private messages for advertising purposes and its ability to provide its service.

Facebook separately argues that, even putting aside the allegations regarding targeted advertising, its interception of users' messages fell within the ordinary course of its business. Facebook argues that the "receipt of its users' electronic messages is in fact necessary to facilitate the transmission of the communications at issue," and thus, the "ordinary course of business" exception would apply even if the court were to apply the Gmail court's narrow view of the exception.

However, at this stage of the case, the court rejects Facebook's attempt to treat its receipt of a user's message and the scanning of that message's content for advertising purposes as part of the same "interception." The court has no evidentiary record regarding the technical details of Facebook's handling of messages, and thus, has no basis to determine whether Facebook's alleged use of a "web crawler" constitutes an "interception" separate from the receipt of the message itself.

At the hearing, Facebook represented that it ceased the challenged practice in October 2012, but confirmed that it still conducts some analysis of the content of users' messages – to protect against viruses, to filter spam messages, and to "protect the integrity of the site." The fact that Facebook can configure its code to scan message content for certain purposes, but not for others, leaves open the possibility that the challenged practice constitutes a separate "interception." Simply put, the application of the "ordinary course of business" exception to this case depends upon the details of Facebook's software code, and those details are simply not before the court on a motion to dismiss, and thus, the court must deny Facebook's motion on that basis. However, the court may re-address the "ordinary course of business" exception at the summary judgment stage of the case, with a more complete evidentiary record before the court.

The court also notes that the Gmail court found the "ordinary course of business" exception inapplicable because the plaintiffs alleged that Google had violated its own internal policies. However, that finding was not critical to the court's rejection of the "ordinary course of business" exception. The Gmail court had already found that Google's interceptions were "neither instrumental to the provision of email services, nor are they an incidental effect of providing these services," and thus, the plaintiffs had "plausibly alleged that the interceptions fall outside Google's ordinary course of business." Gmail at *11. Only after making that finding did the court address the independent argument that Google had violated its own internal policies.

Facebook attempts to persuade the court that, because plaintiffs have not alleged a violation of internal policies in this case, the "ordinary course of business" exception must apply. The court disagrees. While the court does find that plaintiffs have failed to identify a violation of internal policies[1] in this case, that analysis does not affect the above finding that Facebook is not entitled to dismissal based on the ordinary course of business exception.

Finally, the court recognizes the need for the ECPA in general, and the "ordinary course of business" exception in particular, to be read as flexible enough to adapt to technologies that arose long after the statute's passage in 1986. Much of what is "ordinary" today was not at all "ordinary" in 1986, so the scope of the exception cannot be set in stone. The defendant in Gmail raised concern of a "slippery slope" that would "make it impossible for electronic communication service providers to provide basic features, such as email searches or spam filtering." Gmail at *11, n.4. Presumably, Facebook has similar concerns about adding new and innovative features to its service. However, as the Gmail court noted, "a service provider can seek consent to provide features beyond those linked to the provision of the service." Id. In other words, an electronic communication provider

[1]Plaintiffs do not identify any policy which expressly disallows Facebook from scanning its users' messages for their content for advertising purposes. While plaintiffs argue that neither the Data Use Policy nor the Statement of Rights and Responsibilities (both of which are discussed in more detail below) expressly disclose the challenged practice, that is a separate issue from whether any internal policy was affirmatively violated.

need not be concerned that every new feature of its service could trigger Wiretap Act liability – as long as it obtains consent for those features. And, indeed, Facebook does claim that it obtained consent for the interceptions alleged in this case.

b. Consent

If either party to a communication consents to its interception, then there is no violation of the Wiretap Act, "unless such communication is intercepted for the purpose of committing any criminal or tortious act." See 18 U.S.C. § 2511(2)(d). Consent can be either express or implied, and Facebook argues that plaintiffs both expressly and impliedly consented to any alleged interception.

In support of its express consent argument, Facebook points to its "Statement of Rights and Responsibilities" and its "Data Use Policy," both of which must be agreed to by users in order to use the Facebook website. As an initial matter, the court notes that Facebook's motion provides specific citations only to the Data Use Policy, and does not identify any portion of the Statement of Rights and Responsibilities that purportedly establishes consent. The court has reviewed the Statement of Rights and Responsibilities, and finds that it does not establish that users consented to the scanning of their messages for advertising purposes, and in fact, makes no mention of "messages" whatsoever. Instead, it appears that the only relevance of the Statement of Rights and Responsibilities to this case is Facebook's statement that it "encourage[s]" the reader to "read the Data Use Policy, and to use it to help you make informed decisions." Dkt. 42, Ex. A at 1.

The parties have included three versions of the Data Use Policy (in effect at various times during the class period) as part of their joint stipulation regarding judicially noticeable documents.[2] See Dkt. 41, Exs. D-F. The specific language of the policy changes slightly in these three versions, but the general principles remain the same. Facebook informs the user that "we receive data about you whenever you use or are running Facebook," including when you "send or receive a message." Dkt. 41, Ex. D at 2; see also Ex. E at 1,

[2]The court GRANTS the parties stipulation regarding judicially noticeable documents.

Ex. F at 2. As plaintiffs point out, this disclosure is made under a heading called "other information we receive about you."

In another section, titled "how we use the information we receive," Facebook states:

> We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you see. For example, in addition to helping people see and find things that you do and share, we may use the information we receive about you:
>
> 1. as part of our efforts to keep Facebook products, services, and integrations safe and secure;
> 2. to protect Facebook's or others' rights or property;
> 3. to provide you with location features and services, like telling you and your friends when something is going on nearby;
> 4. to measure or understand the effectiveness of ads you and others see, including to deliver relevant ads to you;
> 5. to make suggestions to you and other users on Facebook, such as: suggesting that your friend use our contact importer because you found friends using it, suggesting that another user add you as a friend because the user imported the same email address as you did, or suggesting that your friend tag you in a picture they have uploaded with you in it; and
> 6. for internal operations, including troubleshooting, data analysis, testing, research, and service improvement.

Dkt. 42, Ex. D at 4; see also Ex. E at 2, Ex. F at 4.

When asked, at the hearing, which portion of this policy provided notice of Facebook's practice of scanning users' messages, Facebook's counsel pointed to the disclosure that Facebook "may use the information we received about you" for "data analysis." However, this disclosure is not specific enough to establish that users expressly consented to the scanning of the content of their messages – which are described as "private messages" – for alleged use in targeted advertising[3].

Facebook argues that users have already consented to the messages' "interception" for purposes of facilitating delivery, and thus, Facebook has blanket immunity for any use of

---

[3]As discussed above, Facebook disputes plaintiffs' allegations that users' messages were scanned for the purpose of targeting advertising. However, just as Facebook argued that the allegations of the complaint must be taken as true for the purpose of analyzing its "ordinary course of business" argument, so too must the allegations be taken as true for the purpose of analyzing its "consent" defense.

that information other than for the purpose of committing a criminal or tortious act. However, as discussed above, plaintiffs have alleged that Facebook uses a "web crawler" to scan any URLs that are contained in messages, and to increase the corresponding web page's "like" counter accordingly, and the use of that "web crawler" may constitute a separate "interception" under the Wiretap Act. Accordingly, the court rejects Facebook's argument that plaintiffs expressly consented to the alleged interceptions.

Facebook further argues that plaintiffs impliedly consented to the alleged interceptions. Implied consent may be based on the overall circumstances of a particular communication, and the "critical question with respect to implied consent is whether the parties whose communications were intercepted had adequate notice of the interception." Gmail, 2013 WL 5423918 at *12.

Facebook argues that, "[g]iven the features of the Messages product, plaintiffs had full notice of, necessarily expected, and consented to Facebook's processing of message data." Facebook also emphasizes the "URL preview" feature of Facebook messages, which creates a thumbnail preview of the website whenever a user includes a valid web link in a message.

However, as discussed above in the context of express consent, any consent with respect to the processing and sending of messages itself does not necessarily constitute consent to the specific practice alleged in this case – that is, the scanning of message content for use in targeted advertising. And because the court is without any evidentiary record at this stage of the case, it cannot determine whether the process by which Facebook generates a thumbnail preview is the same process by which it analyzes the URL link to increase the web page's "like" counter. Thus, the court finds that plaintiffs have not impliedly consented to the alleged interception.

Accordingly, the court DENIES Facebook's motion to dismiss plaintiffs' Wiretap Act claim.

2. California's Invasion of Privacy Act

Section 631 of CIPA is the state-law corollary to the Wiretap Act, and creates civil

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 . . . with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts 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; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained. . .

Facebook argues that plaintiffs' claim under section 631 fails for two reasons. First, Facebook argues that plaintiffs consented to any alleged interception. This argument is identical to the "consent" argument addressed above, and the court rejects it for the same reasons.

Second, Facebook argues that plaintiffs' messages could not have been intercepted "in transit," as required by the statute, because the "messages were entirely contained within Facebook's network during the purported 'interception.'" However, plaintiffs' opposition points out that Facebook's messaging function allows users to send messages to non-Facebook email addresses, which shows that the messages cannot be "entirely contained within Facebook's network." Facebook does not address this argument in its reply. Moreover, the complaint's allegation that users' messages were intercepted in transit is to be taken as true at this stage of the case.

Accordingly, the court DENIES Facebook's motion to dismiss plaintiffs' claim under section 631 of CIPA.

Plaintiffs also assert a claim under section 632 of CIPA, which provides for liability against "[e]very person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication."

Facebook again argues that plaintiffs consented to any alleged interception, which the court rejects for the same reasons discussed above. However, Facebook also argues that plaintiffs have not alleged any "confidential communication."

The California Supreme Court has held that a conversation is "confidential" under section 632 "if a party to that conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded." See Kearney v. Salomon Smith Barney, Inc., 39 Cal.4th 95, 117 n.7 (2006); see also Faulkner v. ADT Sec. Services, Inc., 706 F.3d 1017, 1019 (9th Cir. 2013). California appeals courts have generally found that Internet-based communications are not "confidential" within the meaning of section 632, because such communications can easily be shared by, for instance, the recipient(s) of the communications. See, e.g., People v. Nakai, 183 Cal.App.4th 499, 518 (2010). Although Nakai involved an Internet chat, rather than email, the Gmail court found that "email by its very nature is more similar to internet chats" than it is to phone conversations. Gmail, 2013 WL 5423918 at *23. The court finds the reasoning of the Gmail court persuasive, and similarly finds that plaintiffs have not alleged facts leading to the plausible inference that their communications were "confidential" under section 632. Accordingly, Facebook's motion to dismiss plaintiffs' section 632 claim is GRANTED. Because no amendment could establish that plaintiffs' communications were indeed "confidential," plaintiffs shall not be granted leave to amend this claim.

3. Section 17200

California Business & Professions Code section 17200, also referred to as the "Unfair Competition Law" (or "UCL"), prohibits any "unlawful, unfair, or fraudulent business act or practice." A plaintiff seeking to assert a UCL claim must meet the statute's requirements for standing, which are that he or she (1) has suffered an "injury in fact," and (2) "lost money or property." See Kwikset Corp. v. Superior Court, 51 Cal.4th 310, 322 (2011). Facebook argues that plaintiffs fail to meet either requirement.

As to the "injury in fact" requirement, the court notes that the Ninth Circuit recently rejected this argument, finding "a plaintiff demonstrates an injury sufficient to satisfy Article III when bringing a claim under a statute that prohibits the defendant's conduct and grants 'persons in the plaintiff's position a right to judicial relief.'" See In re Zynga Privacy Litigation, 750 F.3d 1098, 1105 n.5 (9th Cir. 2014) (citing Edwards v. First American Corp.,

610 F.3d 514, 517 (9th Cir. 2010)). As discussed above, plaintiffs have established viable claims under the Wiretap Act and under CIPA section 631, which is sufficient to satisfy the "injury in fact" requirement.

However, plaintiffs have not alleged that they have lost any money or property as a result of Facebook's conduct. Plaintiffs argue that they have a property interest in their personal information, including the content of their messages, but courts have consistently rejected such a broad interpretation of "money or property." See, e.g., Opperman v. Path, 2014 WL 1973378 at *23, n.22 (N.D. Cal. May 14, 2014); In re Facebook Privacy Litigation, 791 F.Supp.2d 705, 715 (N.D. Cal. 2011); Claridge v. RockYou, Inc., 785 F.Supp.2d 855, 862 (N.D. Cal. 2011).

Accordingly, Facebook's motion to dismiss plaintiffs' UCL claim is GRANTED without leave to amend.

4. Injunctive relief

Facebook moves to strike plaintiffs' request for injunctive relief, arguing that it ceased the challenged practice "nearly two years ago." However, plaintiffs have adequately alleged that there is a "sufficient likelihood" that Facebook could resume the practice, so the court DENIES Facebook's request to strike the prayer for injunctive relief at this time.

CONCLUSION

For the foregoing reasons, Facebook's motion to dismiss is GRANTED in part and DENIED in part. The motion to dismiss plaintiffs' Wiretap Act claim and CIPA section 631 claim is DENIED, and the motion to dismiss plaintiffs' CIPA section 632 claim and section 17200 claim is GRANTED. Facebook's request to strike plaintiffs' prayer for injunctive relief is DENIED.

IT IS SO ORDERED.

Dated: December 23, 2014

PHYLLIS J. HAMILTON
United States District Judge