Exhibit A

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MATTHEW CAMPBELL, et al.,

Plaintiffs,

v.

FACEBOOK INC.,

Defendant.

Case No. 13-cv-5996-PJH

ORDER GRANTING IN PART AND DENYING IN PART MOTION FOR CLASS CERTIFICATION

United States District Court
Northern District of California

On March 16, 2016, plaintiffs' motion for class certification came on for hearing before this court. Plaintiffs Matthew Campbell and Michael Hurley ("plaintiffs") appeared through their counsel, Michael Sobol, Hank Bates, David Rudolph, and Melissa Gardner. Defendant Facebook, Inc. ("defendant" or "Facebook") appeared through its counsel, Christopher Chorba, Joshua Jessen, Jeana Maute, and Priyanka Rajagopalan. Having read the papers filed in conjunction with the motion and carefully considered the arguments and the relevant legal authority, and good cause appearing, the court hereby rules 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 access their "messages" through an inbox on the Facebook website, akin to an email inbox. This suit arises out of Facebook's handling of these "private messages."

In the operative Consolidated Amended Class Action Complaint ("Complaint"), plaintiffs allege that Facebook scans the content of these private messages for use in connection with its "social plugin" functionality. The "social plugin" operates as follows: 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 in the Complaint 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").

Plaintiffs now move for class certification, but their current class definition differs from the one set forth in the operative complaint. The Complaint is brought on behalf of "[a]ll 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." Complaint, ¶ 59. In their motion, plaintiffs move for certification of the following class: "All natural-person Facebook users located within the United States who

have sent, or received from a Facebook user, private messages that included URLs in their content (and from which Facebook generated a URL attachment), from within two years before the filing of this action up through the date of the certification of the class."[1] Dkt. 138 at 10-11. The key differences are (1) the inclusion of a parenthetical that limits the relevant messages to those "from which Facebook generated a URL attachment," and (2) the removal of the reference to Facebook ceasing the challenged practice.

At the hearing, the court questioned plaintiffs about the incongruity between the Complaint and the class certification motion, and plaintiffs' counsel explained that the changes are the result of new information that was learned through discovery. And in addition to the changes to the class definition, plaintiffs' motion also describes two additional ways in which Facebook allegedly violated the ECPA and CIPA, beyond the one alleged in the Complaint.

As mentioned above, plaintiffs' original theory was that Facebook scans the users' messages, and when a URL was included, it would increase the "Like" counter for that URL. Now, plaintiffs allege two other interceptions/uses[2]: (1) Facebook scans users' messages, and when a URL is included, it uses that data to generate recommendations

[1] Plaintiffs also exclude the following from the class definition: "Facebook and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Facebook has a controlling interest; counsel for the putative class; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and any and all federal, state, or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members." Dkt. 138 at 11.

[2] In its motion to dismiss, Facebook argued that plaintiffs were not challenging the "interception" of their messages, but rather the "use" of those messages. The court cited Ninth Circuit authority defining an "interception" as an "acquisition of the contents" of a communication, and further holding that an "acquisition" occurs "when the contents of a wire communication are captured or redirected in any way." Dkt. 43 at 5 (citing Noel v. Hall, 568 F.3d 743, 751 (9th Cir. 2009)). The court held that there was no evidentiary record from which to conclude that the messages were not "redirected" in order to be used in the manner alleged in the complaint. Plaintiffs' expert has now opined that "Facebook intercepted and redirected user's private message content . . . while the message was in transit," so for purposes of this motion, the court finds that plaintiffs have adequately established that each alleged "use" stemmed from an interception. See Dkt. 137-6, ¶ 17.

for other users[3], and (2) Facebook scans the messages, and when a URL is included, it shares that data with third parties so that they can generate targeted recommendations.

Plaintiffs' motion (and accompanying expert report) describes these two newly-alleged practices, and also sets forth more detailed allegations regarding the "Like" counter increase. Plaintiffs' motion makes clear that these new allegations are derived from a review of Facebook's source code, which had not yet been produced at the time that the operative complaint was filed.

Plaintiffs explain that, when a Facebook user composes a message with a URL in the message's body, Facebook generates a "URL preview," consisting of a brief description of the website and a relevant image from the website, if available. Facebook keeps a record of these "URL previews" – the record being called an "EntShare." The "EntShare" is tied to the specific user who sent the message. Facebook also creates another record called a "EntGlobalShare," which tracks all users who sent a message containing the same URL.

Plaintiffs then specifically describe the three ways in which the message data is allegedly redirected and used. The first is to "fuel its algorithms for measuring user engagement and making recommendations." This alleged use is related to the "EntShare" and the "EntGlobalShare" described above – essentially, Facebook keeps a tally of the number of times that a certain URL has been shared in users' messages (the "EntGlobalShare" number), and then incorporates that number "into secret algorithms that pushed content to users across the social network." As an example, plaintiffs cite to Facebook's "Taste" system, which generates recommendations "to push to targeted

[3] The parties are still disputing the details of this alleged practice, with Facebook filing an "errata" on May 11, 2016 to clarify and withdraw some of the assertions made during briefing, and with plaintiffs filing a response asking the court to strike the errata. The court will not strike Facebook's errata at this time, because it does seek to correct certain representations made previously, but the court's current order does not rely on the errata in any manner. For purposes of this motion, the court finds that plaintiffs have adequately shown that Facebook intercepts users' message data in order to generate recommendations, even as the parties continue to dispute the specifics of those alleged interceptions.

users that Facebook believes the user would find relevant." The recommendations are generated by a piece of source code called "ExternalNodeRecommender," which takes into account which URLs a users' friends had shared (in other words, a user's friends' messages will be weighted more heavily than the messages of random users in generating recommendations). Thus, plaintiffs allege that "Facebook's recommendation system used private message content to target Internet links to specific users."

The second use alleged by plaintiffs is the "sharing of user data with third parties." Plaintiffs argue that Facebook "redirects" the content of private messages to interested third parties through its "Insights" product, allowing those third parties to "help the website customize content for its existing visitors and target advertising to attract new visitors."

The third use alleged by plaintiffs is the "Like" count increase, which was discussed extensively during the motion to dismiss proceedings, and in the court's order resolving that motion. See Dkt. 43. Specifically, when a user sends a message with a URL, Facebook counts that as equivalent to a user actively clicking "like" on the website link. Plaintiffs supplement their earlier allegations regarding this practice with testimony from Facebook employees. For instance, in one exchange, a Facebook employee discusses the "acknowledged problem" that "a shortage of likes is limiting the number of users that can be targeted by their interests and thereby affecting revenue." Dkt. 138-4, Ex. 8. Another employee described the practice of including user message content in this "like" count, saying that "the motivation was to make [the Like count] as big as possible." Dkt. 138-4, Ex. 9.

In another exchange, Facebook CEO Mark Zuckerberg complained in an email that Twitter's numbers for its "like"-equivalent were much higher than Facebook's, and argued that "we should be showing the largest number we can rationalize showing." Dkt. 138-4, Ex. 15. And in yet another exchange, employees discussed the practice of including message scans in the "like" total, and said that "we have intentionally not proactively messaged what this number is since it's kind of sketchy how we construct it." Dkt. 138-4, Ex. 17.

While the Complaint already includes allegations regarding the "Like" counter increase, and arguably includes allegations regarding the interception of messages to generate user recommendations (see Complaint, ¶¶ 49-51), it does not contain allegations regarding the sharing of data with third parties. However, because these allegations are based on a review of discovery that was not available at the time of the complaint's filing, the court finds that plaintiffs are not acting in bad faith by alleging these new facts now. Nor does the court find that Facebook would be prejudiced by the addition of these new allegations. And given that there is not yet a deadline for pleadings to be amended, the court finds that an amendment of the complaint would be appropriate, in order to bring the complaint in line with the allegations, and the class definition, as presented on this motion for class certification. Accordingly, plaintiffs are directed to file an amended complaint, making only the following changes: (1) revising the class definition to reflect the definition set forth in the class certification motion, and (2) adding allegations regarding the sharing of data with third parties. To the extent that plaintiffs seek to make any other amendments to the complaint, they must obtain either leave of court or a stipulation from Facebook.

Turning back to the present motion, plaintiffs seek class certification under Rule 23(b)(3), or in the alternative, under Rule 23(b)(2).

DISCUSSION

A. Legal Standard

"Before certifying a class, the trial court must conduct a 'rigorous analysis' to determine whether the party seeking certification has met the prerequisites of Rule 23." Mazza v. American Honda Motor Co., Inc., 666 F.3d 581, 588 (9th Cir. 2012) (citation and quotation omitted).

The party seeking class certification bears the burden of affirmatively demonstrating that the class meets the requirements of Federal Rule of Civil Procedure 23. Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 350 (2011). In order for a class action to be certified, plaintiffs must prove that they meet the requirements of Federal Rule of

Civil Procedure 23(a) and (b).

Rule 23(a) requires that plaintiffs demonstrate numerosity, commonality, typicality and adequacy of representation in order to maintain a class. First, the class must be so numerous that joinder of all members individually is "impracticable." See Fed. R. Civ. P. 23(a)(1). Second, there must be questions of law or fact common to the class. Fed. R. Civ. P. 23(a)(2). Third, the claims or defenses of the class representative must be typical of the claims or defenses of the class. Fed. R. Civ. P. 23(a)(3). And fourth, the class representative(s) must be able to protect fairly and adequately the interests of all members of the class. Fed. R. Civ. P. 23(a)(4). The parties moving for class certification bear the burden of establishing that the Rule 23(a) requirements are satisfied. Gen'l Tel. Co. of Southwest v. Falcon, 457 U.S. 147, 156 (1982); see also Dukes, 564 U.S. at 350.

If all four prerequisites of Rule 23(a) are satisfied, the court then determines whether to certify the class under one of the three subsections of Rule 23(b), pursuant to which the named plaintiffs must establish either (1) that there is a risk of substantial prejudice from separate actions; or (2) that declaratory or injunctive relief benefitting the class as a whole would be appropriate; or (3) that common questions of law or fact common to the class predominate and that a class action is superior to other methods available for adjudicating the controversy at issue. See Fed. R. Civ. P. 23(b)(3).

The court does not make a preliminary inquiry into the merits of plaintiffs' claims in determining whether to certify a class. Eisen v. Carlisle & Jacquelin, 417 U.S. 156, 177 (1974). The court will, however, scrutinize plaintiffs' legal causes of action to determine whether they are suitable for resolution on a class-wide basis. See, e.g., Moore v. Hughes Helicopters, Inc., 708 F.2d 475, 480 (9th Cir. 1983). Making such a determination will sometimes require examining issues that overlap with the merits. See Dukes, 564 U.S. at 351 (acknowledging that court's "rigorous analysis" will frequently entail some overlap with merits of plaintiff's underlying claim).

B. Legal Analysis

As mentioned above, plaintiffs move for class certification under Rule 23(b)(3),

and in the alternative, under Rule 23(b)(2). While Facebook challenges a number of the requirements under Rule 23(a) and Rule 23(b), it also levies a more overarching challenge based on the alleged "individualized inquiry" needed to determine "whether a particular person was impacted by the challenged practices." While this is primarily an "ascertainability" argument, Facebook attempts to stretch it into an argument against commonality, predominance, and even numerosity. Rather than addressing the argument each time it is raised, the court will fully discuss the ascertainability issue first.

Although Rule 23 makes no mention of an "ascertainability" requirement, courts in this district have found that such a requirement is implied by Rule 23. See, e.g., Mazur v. eBay Inc., 257 F.R.D. 563, 567 (N.D. Cal. 2009) ("apart from the explicit requirements of Rule 23(a), the party seeking class certification must demonstrate that an identifiable and ascertainable class exists"). However, courts have drawn a distinction between Rule 23(b)(2) classes and Rule 23(b)(3) classes, holding that the ascertainability requirement applies to (b)(3) classes, but not to (b)(2) classes. A recent opinion from this district provides a useful explanation of the distinction. See In re Yahoo Mail Litigation, 308 F.R.D. 577 (N.D. Cal. 2015). The Yahoo court first recognized that "the Ninth Circuit has not expressly addressed the issue of whether the judicially implied ascertainability requirement applies when a plaintiff moves to certify a class only under Rule 23(b)(2)." Id. at 597. However, "every other circuit to address the issue has concluded that the ascertainability requirement does not apply to Rule 23(b)(2) cases." Id. (internal citations omitted).

The Yahoo court then explained that the ascertainability requirement arose out of the "additional procedural safeguards" necessary for a (b)(3) class, including that class members be given notice of the class and an opportunity to opt out. In order to provide those safeguards, "the court must be able to ascertain, i.e., identify potential class members." 308 F.R.D. at 597. In contrast, because (b)(2) classes seek declaratory or injunctive relief that is indivisible among the class, "the identities of individual class members are less critical in a (b)(2) action than in a (b)(3) action." Id. (internal citation

omitted); see also Dukes, 564 U.S. at 362 ("The procedural protections attending the (b)(3) class – predominance, superiority, mandatory notice, and the right to opt out – are missing from (b)(2) not because the Rule considers them unnecessary, but because it considers them unnecessary to a (b)(2) class.") (emphasis in original).

Taking into account the purpose behind the ascertainability requirement, the Yahoo court found that "as a matter of practical application, the ascertainability requirement serves little purpose in Rule 23(b)(2) classes, as there will generally be no need to identify individual class members," and as a result, it held that "the ascertainability requirement does not apply to Rule 23(b)(2) actions." 308 F.R.D. at 597. The court finds the Yahoo court's reasoning to be persuasive, and adopts it here. The court also notes that Facebook has not cited any cases applying the ascertainability requirement to a (b)(2) class. Thus, to the extent plaintiffs seek certification of a Rule 23(b)(2) class, they shall not be required to establish ascertainability.

However, plaintiffs also seek certification of a Rule 23(b)(3) class, and must show ascertainability with respect to that proposed class. As mentioned above, Facebook argues that the "individualized inquiry" needed with respect to each message "precludes a finding of ascertainability." Dkt. 178-2 at 11. However, Facebook appears to be combining two distinct arguments here.

First, Facebook argues that not all messages resulted in the creation of an "EntShare" (also referred to as a "share object"). For instance, "if a person only sent or received Facebook messages without a URL, there would be no URL attachment or object." Dkt. 178-2 at 11. Or, if a person "included a URL in the body of a message but sent the message before a URL preview could be generated, or deleted the URL preview before hitting send, then no share object would have been created." Id. Or, if a person composing a message "did not have JavaScript enabled," or if the message included a URL that was on Facebook's list of malicious URLs, or if the message-sender was using a smartphone application to send the message, then "Facebook would not have generated a URL preview or share object." Id. at 11-12. However, in pointing out these

instances where there was "no URL attachment or object," Facebook overlooks the fact that plaintiffs' own class definition specifically carves out these instances:

> All natural-person Facebook users located within the United States who have sent, or received from a Facebook user, private messages that included URLs in their content (and from which Facebook generated a URL attachment), from within two years before the filing of this action up through the date of the certification of the class.

Dkt. 138 at 10-11 (emphasis added).

By limiting the relevant messages to those "from which Facebook generated a URL attachment," plaintiffs have already accounted for the supposed outliers discussed in the previous paragraph. Any messages that did not generate a URL attachment (or share object[4]) have already been excluded from the class definition, and thus, they are not relevant to the class certification analysis. Facebook's arguments would be relevant if plaintiffs had failed to make such an exclusion – but even then, Facebook's arguments would go more to overbreadth than to ascertainability.

However, Facebook also makes a second argument with respect to ascertainability, arguing that there is no reliable means of isolating the messages "from which Facebook generated a URL attachment," and thus, no means of identifying the senders and recipients of those messages. This argument does go to ascertainability, because if plaintiffs cannot identify the senders/recipients of messages containing a URL attachment, they will not be able to provide notice and an opt-out opportunity to those users.

In support of their argument that the class is ascertainable, plaintiffs rely on the testimony of their expert, Dr. Jennifer Golbeck, who opines that the class can be ascertained through a query of Facebook's database records. See Dkt. 137-6, ¶¶ 103-105. Specifically, Dr. Golbeck explains that, when a message is sent with a URL

[4] Facebook's own opposition brief appears to use the term "URL preview" interchangeably with "share object." See Dkt. 178-2 at 7 ("URL previews are stored on Facebook's servers in the form of 'global' share objects"), 8 ("URL preview – i.e., the global share object").

attachment, a share object called an "EntShare" is created in Facebook's source code. See id., ¶¶ 34-42. Each such message has a unique EntShare with a unique numerical identifier, and each EntShare is tied to the Facebook user ID of the message's sender. Id. ¶¶ 98-101. All of this information is stored in a "private message database" called "Titan," and the Titan database contains all of the information needed to identify members of the class. See Dkt. 166-6, ¶¶ 7-9. Specifically, the Titan database shows (1) the date and time that the message was sent, (2) the sender's user ID, (3) the recipient's user ID, and (4) the EntShare ID. Id., ¶ 8. Dr. Golbeck argues that a "database query could be written that would identify the senders and recipients of Private Messages sent during the Class Period with URL attachments," and sets forth the specific steps for doing so in her opening and rebuttal reports. Id., ¶¶ 9-10, see also Dkt. 137-6, ¶¶ 103-105.

Facebook calls Dr. Golbeck's proposal "not only speculative" but also "futile." Facebook points to Dr. Golbeck's deposition testimony, arguing that it undermines the reliability and accuracy of the "database query" method of ascertaining the class. For example, Facebook argues that the database query would not identify message recipients, or message senders whose URLs were blocked as malicious, or senders who had deleted URL attachments. Dkt. 178-2 at 14.

Along with plaintiffs' reply brief, Dr. Golbeck submitted a rebuttal report, addressing each of the concerns identified by Facebook.[5] In general, Dr. Golbeck argues

[5] Facebook objects to Dr. Golbeck's rebuttal report, arguing that it should be stricken. See Dkt. 169-4. The thrust of Facebook's objection is that the rebuttal report refers to the "Titan database," which was not mentioned in Dr. Golbeck's opening report. However, it appears that the rebuttal report simply adds the name of the database, which was referred to simply as a "database" in the original report. See, e.g., Dkt. 137-6, ¶ 103 ("A database query could be used"); see also Dkt. 166-6, ¶ 14 ("Although I did not mention Titan by name in my opening report, I specifically referenced using a database query"). Facebook appears to be overstating the "newness" of the information contained in the rebuttal report, and the request to strike is DENIED. Facebook also requests that, if the report is not stricken, that "Facebook should be permitted to respond via the attached declarations of Facebook engineers Alex Himel and Dale Harrison." However, those declarations contain arguments that could have been raised in response to the opening Golbeck report, and are not dependent on the rebuttal report's invocation of the term "Titan." Thus, Facebook's request is DENIED. Finally, Facebook argues that plaintiffs have included "a number of troubling misstatements of fact in their reply that should be stricken." To the extent that Facebook seeks to challenge alleged "misstatements of

that Facebook's criticisms are "based on an assumption that the Titan database does not exist," even though it is "Facebook's database-of-record for its Private Message service." Dkt. 166-6, ¶ 14. While a query of only the EntShare database may indeed result in the limitations identified by Facebook (because, for instance, the EntShare database does not keep track of message recipients), Dr. Golbeck explains that "Entshares can be queried to determine whether they were created from URLs sent in Private Messages, and thus, combined with the query related to Titan described above which returns the IDs of Entshares associated with specific Private Messages, class members can be readily identified." Id., ¶ 12. Dr. Golbeck further explains that the Titan database contains information about the sender of each class-qualifying message, the recipient of each class-qualifying message, and the timestamp of each class-qualifying message (allowing a determination of whether the message was sent during the class period), among other things. Id., ¶ 8. Also, to the extent that certain messages may have been blocked due to malicious content, or to the extent that senders may have deleted the URL attachment before sending, those messages fall outside the boundaries of the class definition, because no message with a URL attachment was ever actually sent.

Facebook also briefly argues that "even if a share object was created, there is more variability" around the way that each share object was handled by Facebook's system, due to "technical complexities" or other reasons. See Dkt. 178-2 at 13. Facebook's opposition brief does not develop these arguments, instead directing the court to various parts of the voluminous record filed in connection with the opposition brief. This evidence largely points to situations such as "database failures" or "race conditions" (where multiple people share the same URL at the same time) as creating variabilities, but provides no indication of how often they occur. Indeed, Facebook's declarant admits that "[a]s with any system of this size, it is expected that at least some machines will always be offline or not functioning properly resulting in some error." The

---

fact," it must seek leave to file a surreply, it may not simply file an unauthorized surreply under the guise of "objections." That portion of Facebook's filing is therefore stricken.

general proposition that machines sometimes do not function properly cannot be sufficient to defeat ascertainability. Without more, Facebook cannot rebut the showing made by plaintiffs that a method exists for determining who fits within the proposed class. Accordingly, the court finds that the class is objectively ascertainable, and it will now address the Rule 23(a) factors.

1. Rule 23(a)

a. Numerosity

Rule 23(a)(1) requires that a class be so numerous that joinder of all members is impracticable. In order to satisfy this requirement, plaintiffs need not state the "exact" number of potential class members, nor is there a specific number that is required. See In re Rubber Chems. Antitrust Litig., 232 F.R.D. 346, 350-51 (N.D. Cal. 2005). Rather, the specific facts of each case must be examined. In re Beer Distrib. Antitrust Litig., 188 F.R.D. 557, 561 (N.D. Cal. 1999) (citing General Tel. Co. v. EEOC, 446 U.S. 318, 330 (1980)). While the ultimate issue in evaluating this factor is whether the class is too large to make joinder practicable, courts generally find that the numerosity factor is satisfied if the class comprises 40 or more members, and will find that it has not been satisfied when the class comprises 21 or fewer. See, e.g., Consolidated Rail Corp. v. Town of Hyde Park, 47 F.3d 473, 483 (2d Cir. 1995); Ansari v. New York Univ., 179 F.R.D. 112, 114 (S.D.N.Y. 1998).

Facebook does not directly challenge the numerosity of the proposed class, but rather, argues in a footnote that "[b]ecause the proposed class is not ascertainable, plaintiffs also do not meet their burden of showing Rule 23(a)(1) numerosity." Dkt. 178-2 at 14, n.8. Because the court has found that the class is objectively ascertainable, the court finds no basis for this challenge. Instead, the court looks to plaintiffs' representation that, in 2012, Facebook had approximately 600 million monthly active users of the private message function. Although this number is a worldwide total, given the relatively low bar for finding numerosity, the court finds that the proposed class is sufficiently numerous for Rule 23(a) purposes.

b. Commonality

Rule 23(a)(2) requires "questions of law or fact common to the class." This provision requires plaintiffs to "demonstrate that the class members 'have suffered the same injury,'" not merely violations of "the same provision of law." Dukes, 564 U.S. at 349-50 (internal citation omitted). Accordingly, plaintiffs' claims "must depend upon a common contention" such that "determination of [their] truth or falsity will resolve an issue that is central to the validity of each one of the claims in one stroke." Id. "What matters to class certification . . . is not the raising of common 'questions' – even in droves – but, rather the capacity of a classwide proceeding to generate common answers apt to drive the resolution of the litigation." Id. (internal citation omitted).

Plaintiffs need not show, however, that "every question in the case, or even a preponderance of questions, is capable of class wide resolution. So long as there is 'even a single common question,' a would-be class can satisfy the commonality requirement of Rule 23(a)(2)." Wang v. Chinese Daily News, Inc., 737 F.3d 538, 544 (9th Cir. 2013) (quoting Dukes, 564 U.S. at 359); see also Mazza, 666 F.3d at 589 ("commonality only requires a single significant question of law or fact"). Thus, "[w]here the circumstances of each particular class member vary but retain a common core of factual or legal issues with the rest of the class, commonality exists." Evon v. Law Offices of Sidney Mickell, 688 F.3d 1015, 1029 (9th Cir. 2012) (citations and quotations omitted).

Plaintiffs argue that proof of the elements of the ECPA and CIPA is necessarily common, because it will focus on Facebook's uniform conduct, such as its internal operations and source code, and its interception and redirection of messages.

Facebook responds by arguing that the "'interceptions' did not occur in all cases, nor did they apply uniformly," and instead, "[f]or any particular Facebook message, it would be necessary to determine whether (1) a share object was created, (2) the anonymous, aggregate counter in the global share object was incremented, and (3) the URL scrape or share was 'logged.'" Dkt. 178-2 at 18.

Facebook appears to overstate the showing needed to establish commonality. As explained above, even a single common question is sufficient. Thus, the mere fact that Facebook creates a share object every time a message is sent with a URL is sufficient to establish commonality. Any individual differences between those messages are properly considered as part of the predominance requirement of Rule 23(b)(3).

c. Typicality

The third requirement under Rule 23(a) is that the claims or defenses of the class representatives must be typical of the claims or defenses of the class. Fed. R. Civ. P. 23(a)(3). Typicality exists if the named plaintiffs' claims are "reasonably coextensive" with those of absent class members. Staton v. Boeing, 327 F.3d 938, 957 (9th Cir. 2003). To be considered typical for purposes of class certification, the named plaintiff need not have suffered an identical wrong. Id. Rather, the class representative must be part of the class and possess the same interest and suffer the same injury as the class members. See Falcon, 457 U.S. at 156.

"The purpose of the typicality requirement is to assure that the interest of the named representative aligns with the interests of the class." Hanon v. Dataproducts Corp., 976 F.2d 497, 508 (9th Cir. 1992) (citation omitted). According to the Ninth Circuit, "[t]ypicality refers to the nature of the claim or defense of the class representative, and not to the specific facts from which it arose or the relief sought." Id. (quotation omitted). "The test of typicality is whether other members have the same or similar injury, whether the action is based on conduct which is not unique to the named plaintiffs, and whether other class members have been injured by the same course of conduct." Id. (internal quotation marks omitted); see also Armstrong v. Davis, 275 F.3d 849, 868 (9th Cir. 2001) (typicality is satisfied when each class member's claim arises from the same course of events, and each class member makes similar legal arguments to prove the defendant's liability); Lightbourn v. County of El Paso, 118 F.3d 421, 426 (5th Cir. 1997) (typicality focuses on the similarity between the named plaintiffs' legal and remedial theories and the legal and remedial theories of those whom they purport to represent). In practice, the

commonality and typicality requirements of Rule 23 "tend to merge." Falcon, 457 U.S. at 158 n. 13. The Ninth Circuit interprets the typicality requirement permissively. Hanlon v. Chrysler Corp., 150 F.3d 1011, 1020 (9th Cir. 1998).

Plaintiffs argue that they are Facebook users who have sent private messages containing a URL link, and that Facebook intercepted the URL content of their messages in the same manner that it did with the rest of the class's messages. Facebook does not rebut plaintiffs' arguments as to typicality, and the court finds that the typicality requirement is met.

d. Adequacy

The fourth requirement under Rule 23(a) is adequacy of representation. The court must find that named plaintiffs' counsel is adequate, and that named plaintiffs can fairly and adequately protect the interests of the class. To satisfy constitutional due process concerns, unnamed class members must be afforded adequate representation before entry of a judgment which binds them. See Hanlon, 150 F.3d at 1020. Legal adequacy is determined by resolution of two questions: (1) whether named plaintiffs and their counsel have any conflicts with class members; and (2) whether named plaintiffs and their counsel will prosecute the action vigorously on behalf of the class. Id. Generally, representation will be found to be adequate when the attorneys representing the class are qualified and competent, and the class representatives are not disqualified by interests antagonistic to the remainder of the class. Lerwill v. Inflight Motion Pictures, 582 F.2d 507, 512 (9th Cir. 1978).

Plaintiffs argue that they have no antagonism with class members' interests and that they have committed to prosecute the case vigorously on behalf of all class members. They argue that plaintiffs' counsel have substantial experience in litigating privacy claims, and will commit the resources necessary to represent the class.

Facebook argues that neither plaintiffs nor their counsel are adequate for three reasons. First, Facebook argues that this suit "was initiated and is driven by class counsel." Second, Facebook argues that "plaintiffs' close relationships with class

counsel" render them inadequate class representatives. And finally, Facebook argues that plaintiffs' counsel's "mistreatment" of a former plaintiff in this case should "disqualify" them from serving as class counsel. The court finds each of these concerns to be overstated.

The first two arguments rely on the speculative notion that plaintiffs will be unduly influenced by their attorneys into taking positions that run counter to the interests of the class members. However, Facebook points to no actual conflict between the putative class members and the proposed class representatives/counsel. See Cummings v. Connell, 316 F.3d 886, 896 (9th Cir. 2003) ("this circuit does not favor denial of class certification on the basis of speculative conflicts").

As to the third argument, the court finds that Facebook has blurred the distinction between the proposed class counsel and the counsel of former plaintiff David Shadpour. For instance, Facebook argues that Mr. Shadpour "did not review or receive his original complaint before it was filed." However, former plaintiff Shadpour's original complaint was filed by different counsel than those representing plaintiffs Campbell and Hurley on this motion. See Case no. 14-cv-0307, Dkt. 1 (N.D. Cal. Jan. 21, 2014) (original complaint in Shadpour v. Facebook, Inc.). While Mr. Shadpour's deposition testimony also indicates that he did not review the consolidated complaint filed in this action, plaintiffs provide a declaration stating that the consolidated complaint was provided to Mr. Shadpour's former counsel, so any failure to review it cannot be attributable to the putative class counsel. In short, the court finds no indication that either plaintiffs or their counsel has any conflict with the class members, nor any reason to believe that they would not prosecute the action vigorously on behalf of the class. Accordingly, the court finds the adequacy requirement to be met.

2. Rule 23(b)

As mentioned above, Rule 23(b)(3) requires the party seeking class certification to show that "questions of law or fact common to class members predominate over questions affecting only individual members," and that class treatment is "superior to

other available methods for fairly and efficiently adjudicating the controversy."

a. Predominance

The requirement that questions of law or fact common to class members predominate over questions affecting only individual members "tests whether proposed classes are sufficiently cohesive to warrant adjudication by representation." Amchem Prods., Inc. v. Windsor, 521 U.S. 591, 623 (1997). This inquiry requires the weighing of the common questions in the case against the individualized questions, which differs from the Rule 23(a)(2) inquiry as to whether the plaintiff can show the existence of a common question of law or fact. See Dukes, 564 U.S. at 358.

In addition, however, Rule 23(b)(3) requires a more stringent analysis than does Rule 23(a)(2). See Comcast Corp. v. Behrend, 133 S.Ct. 1426, 1432 (2013). Rule 23(a)(2) simply requires a "common contention" that is "capable of classwide resolution" and "will resolve an issue that is central to the validity of each one of the claims in one stroke." Amchem, 521 U.S. at 624; see also Comcast, 133 S.Ct. at 1432; Dukes, 564 U.S. at 350. By contrast, to satisfy the Rule 23(b)(3) predominance inquiry, it is not enough to establish that common questions of law or fact exist, as it is under Rule 23(a)(2)'s commonality requirement. Indeed, the analysis under Rule 23(b)(3) "presumes that the existence of common issues of fact or law have been established pursuant to Rule 23(a)(2)." Hanlon, 150 F.3d at 1022. Rule 23(b)(3) focuses on the "relationship between the common and individual issues." Id. Under the predominance inquiry, "there is clear justification for handling the dispute on a representative rather than an individual basis" if "common questions present a significant aspect of the case and they can be resolved for all members of the class in a single adjudication . . . ." Id., quoted in Mazza, 666 F.3d at 589. An essential part of the predominance test is whether "adjudication of common issues will help achieve judicial economy." In re Wells Fargo Home Loan Mortg. Overtime Pay Litig., 571 F.3d 953, 958 (9th Cir. 2009) (citations and quotations omitted).

Thus, to satisfy this requirement, plaintiffs must show both (1) that the existence of individual injury arising from the defendant's alleged actions (i.e., the defendant's liability

to each class member) is "capable of proof at trial through evidence . . . common to the class rather than individual to its members" and (2) that "the damages resulting from that injury [are] measurable 'on a class-wide basis' through the use of a 'common methodology.'" Comcast, 133 S.Ct. at 1430 (citation omitted).

Plaintiffs argue that "resolution of the common issues – whether Facebook's programmed, uniform treatment of users who send private messages containing URLs or Internet links violates ECPA and CIPA – can be achieved in this one proceeding." Plaintiffs point out that the relevant issues under the ECPA are whether Facebook intercepted its users' messages while in transit, and whether such interception was conducted in the ordinary course of business, and argue that both issues are susceptible to common proof, such as Facebook's source code. Plaintiffs further argue that "the core issues under the CIPA mirror the issues applicable to the ECPA claim," and point out that Facebook's terms of service provide that California law applies to any claim between Facebook and its users.

Facebook argues that the ECPA covers only interceptions of the "contents" of a message, as opposed to the "record information" contained in a message. This distinction is set forth in the ECPA, which allows an electronic communications provider to "divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)." 18 U.S.C. § 2702(c). The statute defines such "record" information to include the "name," "address," and "subscriber number or identity" of the customer. 18 U.S.C. § 2703(c).

As applied to this case, Facebook argues that "[d]etermining whether the URLs constituted the 'contents' of a communication will require a URL-by-URL, message-by-message, sender-by-sender analysis." Dkt. 178-2 at 23. Facebook's position appears to be based on a Ninth Circuit case holding that certain header information, including "the user's Facebook ID and the address of the webpage from which the user's HTTP request to view another webpage was sent," did not constitute the "contents" of a message. In re Zynga Privacy Litigation, 750 F.3d 1098, 1107 (9th Cir. 2014). However, the URLs sent

in this case are nothing like the URLs sent in Zynga. In Zynga, the URL represented the "address of the webpage the user was viewing before clicking on the game icon" that triggered the sending of the message, and the court found that webpage to function "like an 'address,'" rather than as the "substance, purport, or meaning" of a communication. In the messages at issue in this case, the sender is affirmatively choosing to share a certain webpage with the recipient, and the webpage itself is the "substance, purport, or meaning" of the message. The fact that the substance of the message happens to be in the form of a URL does not transform it from "content" to "record information." Indeed, Facebook's argument is undermined by its own practice of creating a URL preview – if the URL represented only "record information," then why would Facebook create a "preview" of it for the recipient to view? In short, the court finds no basis for finding that even one of the relevant messages contained a URL that constituted "record information" rather than "contents," and thus, the "contents" issue provides no barrier to the predominance requirement.

Plaintiffs also point out that both the ECPA and CIPA require that the alleged interception occur without consent, and they argue that the class members' lack of consent will be established through common proof. Facebook focuses on the issue of implied consent, arguing that it requires an individual user-by-user inquiry to determine whether class members impliedly consented to the alleged interceptions.

For support, Facebook primarily relies on an opinion from this district, In re Google Gmail Litigation, 2014 WL 1102660 (N.D. Cal. Mar. 8, 2014) (referred to as "Gmail"). The allegations in Gmail are similar to those in this case – plaintiffs challenged Google's practice of scanning the content of users' email messages. After denying a motion to dismiss, the Gmail court ultimately denied certification under Rule 23(b)(3), finding that "individual issues of consent are likely to predominate over any common issues." Id. at *13. While the court rested this finding on both express consent and implied consent, only implied consent is relevant to this motion.

The Gmail court found that implied consent is "an intensely factual question that

requires consideration of the circumstances surrounding interception to divine whether the party whose communication was intercepted was on notice that the communication would be intercepted." Gmail at *16. However, the court noted that it rejected Google's prior argument that "all email users impliedly consented to Google's interceptions . . . because all email users understand that such interceptions are part and parcel of the email delivery process." Id. Instead, the court was required to consider "what evidence Google can use to argue to the finder of fact that email users have impliedly consented" to the interceptions.

The court then went through the specific evidence cited by Google as establishing implied consent. First, there was a page on the Google website itself stating that "the ads you see may be based on . . . factors like the messages in your mailbox." Second, the same page also gave an example of a user who received lots of messages about photography and cameras, and then was shown an ad for a local camera store. Third, the ads themselves contained buttons that said "Why This Ad?", and if the user clicked on the button, they would be told "this ad is based on emails from your inbox." Fourth, another page on the Google website said that "Google scans the text of Gmail messages in order to filter spam and detect viruses," and "also scans keywords in users' email which are then used to match and serve ads." The Gmail court also cited similar disclosures from non-Google sources, such as newspaper reports. Based on that showing, the Gmail court found that some class members likely viewed those disclosures, and some did not, creating individual issues regarding consent.

While Facebook relies on the ultimate holding of Gmail, the evidence in this case is a far cry from the evidence cited in that case. Facebook cites to only one example of a Facebook-generated document where the message scanning practice was disclosed – in a guide intended for website developers, rather than in Facebook's own terms of service. In fact, plaintiffs suggest that Facebook was actively trying to hide the practice, citing evidence showing that its own employees described the practice as "sketchy" and "downright misleading" and contrary to "the understanding of 99.9% of people." Dkt. 138-

4, Ex. 27, 28. And when faced with a "high degree of scrutiny from privacy advocates," the decision was made to "just remove it." Dkt. 138-4, Ex. 16.

That said, Facebook is correct that one of the alleged practices (the "Like" counter increase) was reported on in 2012, even though the reports came from non-Facebook sources. The Gmail court rejected any distinction between information gleaned from Google sources versus non-Google sources, and this court similarly finds no reason for such a distinction. Gmail at *19. Even if Facebook hid its practice, as long as users heard about it from somewhere and continued to use the relevant features, that can be enough to establish implied consent. The court also notes that the class period has been defined to extend "up through the date of the certification of the class," so the 2012 news reports regarding the "Like" counter increase are relevant to the implied consent analysis.

However, there is an important point that is completely glossed over by Facebook – the public disclosures were limited to the "Like" counter increase, even though plaintiffs now challenge three distinct interceptions/uses of the message content, only one of which is the Like counter increase. As discussed above, plaintiffs also argue that Facebook used the "share objects" in order to make recommendations to other users, and that Facebook shared message data with third parties. While the court finds that individual issues of implied consent do predominate in the context of increasing the Like counter (due to the media reports on the practice), the court does not reach the same conclusion with respect to the other two alleged practices, neither of which were disclosed by either Facebook sources or non-Facebook sources.

Facebook's only statement regarding those two challenged practices is that "[a]ll of these practices varied over time and with different user behavior, and none continue to involve URLs shared in messages." Dkt. 178-2 at 10, n. 6. That sentence is so vague as to be irrelevant to the implied consent analysis. Facebook points to no source of information – either internal or external – where the two challenged practices were disclosed to Facebook users. While it is ultimately plaintiffs' burden to show that common issues predominate over individual ones, if plaintiffs have made such a showing,

it falls to Facebook to rebut that showing and to present the court with a basis for reaching the opposite result. And while Facebook does invoke implied consent as a defense that could potentially raise individual issues, based on the current state of the evidence, those individual issues remain just that – potential. This dearth of evidence regarding implied consent stands in stark contrast to the extensive evidence cited by the Gmail court, leaving the court no basis to find, as the Gmail court did, that "some class members likely viewed some of these . . . disclosures." See Gmail at *18 ("there is a panoply of sources from which email users could have learned of Google's interceptions").

While the court finds that individual issues of implied consent do not predominate over common ones, at least as to two of the alleged practices, that finding does not end the predominance analysis under Rule 23(b)(3). The court must also consider whether individual issues surrounding damages predominate over common issues, or in other words, that "damages are capable of measurement on a classwide basis." See Comcast, 133 S.Ct. at 1433.

The ECPA provides that "the court may assess as damages whichever is the greater of: (A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or (B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000." 18 U.S.C. § 2250(c)(2). CIPA provides for statutory damages, but not damages based on plaintiff's harm or defendant's profits. Cal. Penal Code § 632.7.

Plaintiffs do not appear to seek any sum for "actual damages" that they suffered, but instead, seek damages measured by profits made by Facebook (under ECPA) and/or statutory damages (under ECPA and CIPA). The court will start by addressing plaintiffs' model for damages based on Facebook's profits.

As a threshold matter, plaintiffs attempt to subtly expand the scope of available damages by tweaking the language of the statute. After quoting the ECPA's provision for damages based on "profits made by the violator as a result of the violation," plaintiffs

argue that they can offer "common proof to calculate the value which Facebook derived from intercepting private message content." See Dkt. 138 at 22. While the "value" derived by Facebook may bear some correlation with the "profits made," the terms are not synonymous.

The report of plaintiffs' damages expert takes similar liberties. Under the heading titled "The Measure of Damages," plaintiffs' expert sets forth two categories: (1) "Benefits Resulting from Enhancing the Social Graph by Incorporating Intercepted Data," and (2) "Benefits from Inflating the Like Count on Third Party Websites." See Dkt. 137-3, Ex. E. And while plaintiffs' expert does attempt to tie the value of Facebook's "Social Graph" to its actual advertising profits, he makes no such attempt with respect to the Like Counter. As to the Like Counter, plaintiffs' expert opines that "the economic benefit derived by Facebook . . . lies between two bounds: a higher bound represented by the cost that client websites saved by not having to acquire additional 'Likes' . . . and a lower bound determined by the market value of artificially acquired 'Likes' for pages made possible by manipulating the counting system." Id. at ¶ 62. Neither the higher bound nor the lower bound are tied to Facebook's own actual revenue or profits, and instead, are presented in terms of costs savings to advertisers. While plaintiffs' expert theorizes that "the cost savings to advertisers from the accrual of Likes from the intercepted messages [] were, in principle, made available to spend on additional Facebook marketing campaigns," there appears to be no indication, other than speculation, that the advertisers' cost savings actually did result in additional profits for Facebook. Thus, even in the aggregate, the connection between the Like counter increase and Facebook's profits is too attenuated to support a classwide damages award.[6]

Turning back to the Social Graph, the key flaw underlying plaintiffs' expert's methodology is that it assumes that every message intercepted by Facebook resulted in

[6] As discussed above, the issues regarding implied consent to the "Like" counter increase already preclude class certification, but the damages issues provide an independent basis for denying certification as to that accused practice.

an equal amount of profit to Facebook. The expert's methodology essentially calculates a value for Facebook's Social Graph as a whole (which is the "aggregation of the collected information from all users in general"), then attempts to isolate the "incremental value of Facebook's benefits from enhancing the Social Graph by including data intercepted in private messages." Dkt. 137-3, Ex. E at ¶¶ 35-36. In other words, plaintiffs' expert attempts to calculate what percentage of the Social Graph's value is attributable to the practices at issue in this case. So far, while calculating "incremental value" is certainly not an exact science and must rely on certain assumptions, the court finds no significant flaws in this part of the analysis.

However, the next step of the damages methodology requires calculation of individual damages awards, and it is here where plaintiffs' expert's report falls short. Essentially, plaintiffs' expert relies on the assumption that, because Facebook derives value (and therefore profit) from its Social Graph, and because part of the Social Graph is constructed based on information gleaned from the challenged interceptions, then each challenged interception resulted in an equal amount of profit to Facebook. While this assumption has the benefit of expediency, as it would lead to a straightforward damages distribution, it makes no attempt to actually calculate the profit attributable to each individual interception. And while the court is aware of the difficulty, if not impossibility, of discerning how much of a company's profits is attributable to individual interceptions, and does not intend to foreclose all privacy-related class actions under Rule 23(b)(3), the court's finding simply illustrates the difficulty of calculating non-statutory damages under the ECPA. Indeed, statutory damages are designed to cover situations exactly like this, where actual damages are "uncertain and possibly unmeasurable." See Kehoe v. Fidelity Fed. Bank & Trust, 421 F.3d 1209, 1213 (11th Cir. 2005). Thus, the same difficulty that led to the creation of statutory damages also prevents plaintiffs from establishing a classwide method of awarding damages based on Facebook's profits.

However, as mentioned above, statutory damages remain available to plaintiffs under either ECPA or CIPA. And while statutory damages awards largely avoid the

individualized inquiries that plague awards based on actual damages, statutory damages are not to be awarded mechanically. In fact, the ECPA "makes the decision of whether or not to award damages subject to the court's discretion." DirecTV, Inc. v. Huynh, 2005 WL 5864467, at *8 (N.D. Cal. May 31, 2005) (aff'd by 503 F.3d 847 (9th Cir. 2007)). Such discretion is clear from the statute, which was amended in 1986 to state that the court "may" award damages, rather than stating that it "shall" award damages. However, the court's discretion is limited to deciding whether to "either award the statutory sum or nothing at all," it "may not award any amount between those two figures." Id. at *6.

When exercising that limited discretion, courts have weighed several factors, including: (1) the severity of the violation, (2) whether or not there was actual damage to the plaintiff, (3) the extent of any intrusion into the plaintiff's privacy, (4) the relative financial burdens of the parties, (5) whether there was a reasonable purpose for the violation, and (6) whether there is any useful purpose to be served by imposing the statutory damages amount. DirecTV v. Huynh, 2005 WL 5864467 at *8; Dish Network LLC v. Gonzalez, 2013 WL 2991040, at *8 (E.D. Cal. June 14, 2013). While some of these factors can be analyzed in a manner common to the class (such as "whether there was a reasonable purpose for the violation" and "whether there is any useful purpose to be served by imposing the statutory damages amount"), other factors would warrant individualized analyses. For instance, the "severity of the violation" and the "extent of any intrusion into the plaintiff's privacy" would depend on such facts as how many interceptions any given class member was subjected to and how that class member's messages were intercepted. Even more critically, the question of "whether or not there was actual damage to the plaintiff" would vary between class members, and would be answered in the negative for many class members, including one of the named plaintiffs. See Appendix at 482 (deposition testimony from plaintiff Hurley stating that he is not aware of any economic harm that he suffered).

Overall, the court is persuaded by the fact that many class members appear to have suffered little, if any, harm, such that a statutory damages award would be a

disproportionate penalty. To be clear, it is not the size of an aggregate damages award that the court finds disproportionate – the size of an aggregate statutory damages award is not a proper consideration on a class certification motion. Bateman v. American Multi-Cinema, Inc., 623 F.3d 708, 721-23 (9th Cir. 2010). Rather, it is the fact that many individual damages awards would be disproportionate, and sorting out those disproportionate damages awards would require individualized analyses that would predominate over common ones. If there was a basis to find that every class members' statutory damages award would be equally excessive, then the court could follow the scenario set forth by the Ninth Circuit in Bateman and wait until after damages are awarded before deciding whether to reduce the award as unconstitutionally excessive. See id. at 723. However, as mentioned above, the decision about whether or not to reduce an excessive damages award would necessarily involve individual questions about whether each specific class member's award was excessive. For that reason, the court finds that individual issues regarding damages would predominate over common ones, regardless of whether plaintiffs seek statutory damages or damages based on Facebook's profits. Accordingly, plaintiffs' motion for class certification under Rule 23(b)(3) is DENIED.

b. Superiority

Having already found that the predominance requirement is not met, the court need not reach the "superiority" prong of Rule 23(b)(3).

2. Rule 23(b)(2)

To have a class certified under Rule 23(b)(2), plaintiffs must show that "the party opposing the class has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole." The "predominance" and "superiority" requirements of Rule 23(b)(3) do not apply to Rule 23(b)(2) classes. Instead, "[i]t is sufficient if class members complain of a pattern or practice that is generally applicable to the class as a whole. Even if some class members have not been injured by the challenged practice, a

class may nevertheless be appropriate." Walters v. Reno, 145 F.3d 1032, 1047 (9th Cir. 1998).

Plaintiffs argue that Facebook has "utilized a uniform system architecture and source code to intercept and catalog its users' private message content," and thus, has "acted or refused to act on grounds generally applicable to the class."

Facebook's primary argument against (b)(2) certification is that the class is not "indivisible" because "individual proof will show that many putative class members impliedly consented to the challenged practices." Facebook also argues that some class members may have "welcome[d]" the challenged scanning practices, showing that an injunction would not affect the class in the same way.

The arguments raised by Facebook are very similar to those addressed – and rejected – by the court in Yahoo Mail. 308 F.R.D. at 598-601. Yahoo, like Facebook, argued that the requested injunctive relief was "not 'indivisible' because Yahoo would have to determine consent on an individual basis." Id. at 600. However, the court held that Yahoo "misunderstands the 'indivisibility' requirement," which precludes certification only where "each individual class member would be entitled to a different injunction or declaratory judgment against the defendant." Id. (citing Dukes, 564 U.S. at 360). The Yahoo court cited the Ninth Circuit's holding that "the mere fact that a class member's entitlement to relief might differ from individual to individual did not render the requested injunctive relief improperly divisible." Id. (citing Rodriguez v. Hayes, 591 F.3d 1105, 1125-26 (9th Cir. 2009). Instead, "the fact that the plaintiffs sought relief from a single practice was sufficient to satisfy the indivisibility requirement." Id. (citing Rodriguez at 1125-26). The court also notes that, to the extent that Facebook raises implied consent as an issue requiring individual inquiries, that issue is irrelevant to the Rule 23(b)(2) analysis, which does not ask whether common issues predominate over individual ones. Many of other issues regarding "variabilities" between class members that would be relevant under the (b)(3) analysis (either as part of the predominance requirement or the ascertainability requirement) are irrelevant under the (b)(2) analysis.

The Yahoo court also held that "the fact that some class members might not want Yahoo to cease its interception and scanning . . . does not render plaintiffs' Rule 23(b)(2) class improper." 308 F.R.D. at 601. The court emphasized that "Yahoo does not argue that class members are no longer subject to its interception and scanning practices and would therefore not benefit from the requested relief, but instead asserts that some class members might not want the requested relief." Id. And because the "cases on which Yahoo relies involved situations where class members were no longer subject to the defendant's alleged wrongful conduct and would therefore no longer benefit from the requested relief," those cases were inapposite, and presented no basis for denying (b)(2) certification.

Facebook also separately argues that the "primary relief sought by plaintiffs is monetary relief, not injunctive relief," thus making Rule 23(b)(2) certification inappropriate. However, plaintiffs have represented that they seek "only declaratory and injunctive relief in the alternative request for certification pursuant to Rule 23(b)(2)." The court similarly finds that, to the extent plaintiffs sought monetary damages, those damages were sought pursuant to a Rule 23(b)(3) class. The court construes plaintiffs' alternative request for Rule 23(b)(2) certification as seeking only injunctive and declaratory relief, and for the reasons discussed above, plaintiffs' motion for (b)(2) certification is GRANTED.

CONCLUSION

For the foregoing reasons, plaintiffs' motion for class certification is DENIED as to the proposed Rule 23(b)(3) class, and GRANTED as to the proposed Rule 23(b)(2) class.

As mentioned above, plaintiffs are granted leave to amend the complaint on a limited basis, and any amended complaint must be filed no later than **June 8, 2016**.

Finally, the court will conduct a case management conference on **June 30, 2016** at **2:00 p.m.**

IT IS SO ORDERED.

Dated: May 18, 2016

PHYLLIS J. HAMILTON
United States District Judge