

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

1 privately, with just one other Facebook user, through the use of a “private message.”
2 While not identical to email, a private message is analogous to email, in that it involves
3 an electronic message sent from one user to one or more other users. Facebook users
4 access their “messages” through an inbox on the Facebook website, akin to an email
5 inbox. This suit arises out of Facebook’s handling of these “private messages.”

6 In the operative Consolidated Amended Class Action Complaint (“Complaint”),
7 plaintiffs allege that Facebook scans the content of these private messages for use in
8 connection with its “social plugin” functionality. The “social plugin” operates as follows:
9 certain websites have a Facebook “like” counter displayed on their web pages, which
10 enables visitors of the page to see how many Facebook users have either clicked a
11 button indicating that they “like” the page, or have shared the page on Facebook. In
12 essence, the “like” counter is a measure of the popularity of a web page.

13 Plaintiffs allege in the Complaint that Facebook scans the content of their private
14 messages, and if there is a link to a web page contained in that message, Facebook
15 treats it as a “like” of the page, and increases the page’s “like” counter by one. Plaintiffs
16 further allege that Facebook uses this data regarding “likes” to compile user profiles,
17 which it then uses to deliver targeted advertising to its users. Plaintiffs allege that the
18 messaging function is designed to allow users to communicate privately with other users,
19 and that Facebook’s practice of scanning the content of these messages violates the
20 federal Electronic Communications Privacy Act (“ECPA,” also referred to as the “Wiretap
21 Act”), as well as California’s Invasion of Privacy Act (“CIPA”).

22 Plaintiffs now move for class certification, but their current class definition differs
23 from the one set forth in the operative complaint. The Complaint is brought on behalf of
24 “[a]ll natural-person Facebook users located within the United States who have sent or
25 received private messages that included URLs in their content, from within two years
26 before the filing of this action up through and including the date when Facebook ceased
27 its practice.” Complaint, ¶ 59. In their motion, plaintiffs move for certification of the
28 following class: “All natural-person Facebook users located within the United States who

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

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

13 As mentioned above, plaintiffs’ original theory was that Facebook scans the users’
 14 messages, and when a URL was included, it would increase the “Like” counter for that
 15 URL. Now, plaintiffs allege two other interceptions/uses²: (1) Facebook scans users’
 16 messages, and when a URL is included, it uses that data to generate recommendations
 17

18
 19 ¹ Plaintiffs also exclude the following from the class definition: “Facebook and its parents,
 20 subsidiaries, affiliates, officers and directors, current or former employees, and any entity
 21 in which Facebook has a controlling interest; counsel for the putative class; all individuals
 22 who make a timely election to be excluded from this proceeding using the correct
 23 protocol for opting out; and any and all federal, state, or local governments, including but
 24 not limited to their departments, agencies, divisions, bureaus, boards, sections, groups,
 25 counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation,
 26 as well as their immediate family members.” Dkt. 138 at 11.

27 ² In its motion to dismiss, Facebook argued that plaintiffs were not challenging the
 28 “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.

1 for other users³, and (2) Facebook scans the messages, and when a URL is included, it
2 shares that data with third parties so that they can generate targeted recommendations.

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

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

15 Plaintiffs then specifically describe the three ways in which the message data is
16 allegedly redirected and used. The first is to "fuel its algorithms for measuring user
17 engagement and making recommendations." This alleged use is related to the
18 "EntShare" and the "EntGlobalShare" described above – essentially, Facebook keeps a
19 tally of the number of times that a certain URL has been shared in users' messages (the
20 "EntGlobalShare" number), and then incorporates that number "into secret algorithms
21 that pushed content to users across the social network." As an example, plaintiffs cite to
22 Facebook's "Taste" system, which generates recommendations "to push to targeted
23

24 _____
25 ³ The parties are still disputing the details of this alleged practice, with Facebook filing an
26 "errata" on May 11, 2016 to clarify and withdraw some of the assertions made during
27 briefing, and with plaintiffs filing a response asking the court to strike the errata. The
28 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.

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

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

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

22 In another exchange, Facebook CEO Mark Zuckerberg complained in an email
23 that Twitter’s numbers for its “like”-equivalent were much higher than Facebook’s, and
24 argued that “we should be showing the largest number we can rationalize showing.” Dkt.
25 138-4, Ex. 15. And in yet another exchange, employees discussed the practice of
26 including message scans in the “like” total, and said that “we have intentionally not
27 proactively messaged what this number is since it’s kind of sketchy how we construct it.”
28 Dkt. 138-4, Ex. 17.

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

17 Turning back to the present motion, plaintiffs seek class certification under Rule
18 23(b)(3), or in the alternative, under Rule 23(b)(2).

19 DISCUSSION

20 A. Legal Standard

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

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

1 Civil Procedure 23(a) and (b).

2 Rule 23(a) requires that plaintiffs demonstrate numerosity, commonality, typicality
3 and adequacy of representation in order to maintain a class. First, the class must be so
4 numerous that joinder of all members individually is “impracticable.” See Fed. R. Civ. P.
5 23(a)(1). Second, there must be questions of law or fact common to the class. Fed. R.
6 Civ. P. 23(a)(2). Third, the claims or defenses of the class representative must be typical
7 of the claims or defenses of the class. Fed. R. Civ. P. 23(a)(3). And fourth, the class
8 representative(s) must be able to protect fairly and adequately the interests of all
9 members of the class. Fed. R. Civ. P. 23(a)(4). The parties moving for class certification
10 bear the burden of establishing that the Rule 23(a) requirements are satisfied. Gen’l Tel.
11 Co. of Southwest v. Falcon, 457 U.S. 147, 156 (1982); see also Dukes, 564 U.S. at 350.

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

19 The court does not make a preliminary inquiry into the merits of plaintiffs’ claims in
20 determining whether to certify a class. Eisen v. Carlisle & Jacquelin, 417 U.S. 156, 177
21 (1974). The court will, however, scrutinize plaintiffs’ legal causes of action to determine
22 whether they are suitable for resolution on a class-wide basis. See, e.g., Moore v.
23 Hughes Helicopters, Inc., 708 F.2d 475, 480 (9th Cir. 1983). Making such a
24 determination will sometimes require examining issues that overlap with the merits. See
25 Dukes, 564 U.S. at 351 (acknowledging that court’s “rigorous analysis” will frequently
26 entail some overlap with merits of plaintiff’s underlying claim).

27 B. Legal Analysis

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

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

8 Although Rule 23 makes no mention of an “ascertainability” requirement, courts in
9 this district have found that such a requirement is implied by Rule 23. See, e.g., Mazur v.
10 eBay Inc., 257 F.R.D. 563, 567 (N.D. Cal. 2009) (“apart from the explicit requirements of
11 Rule 23(a), the party seeking class certification must demonstrate that an identifiable and
12 ascertainable class exists”). However, courts have drawn a distinction between Rule
13 23(b)(2) classes and Rule 23(b)(3) classes, holding that the ascertainability requirement
14 applies to (b)(3) classes, but not to (b)(2) classes. A recent opinion from this district
15 provides a useful explanation of the distinction. See In re Yahoo Mail Litigation, 308
16 F.R.D. 577 (N.D. Cal. 2015). The Yahoo court first recognized that “the Ninth Circuit has
17 not expressly addressed the issue of whether the judicially implied ascertainability
18 requirement applies when a plaintiff moves to certify a class only under Rule 23(b)(2).”
19 Id. at 597. However, “every other circuit to address the issue has concluded that the
20 ascertainability requirement does not apply to Rule 23(b)(2) cases.” Id. (internal citations
21 omitted).

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

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

5 Taking into account the purpose behind the ascertainability requirement, the
6 Yahoo court found that “as a matter of practical application, the ascertainability
7 requirement serves little purpose in Rule 23(b)(2) classes, as there will generally be no
8 need to identify individual class members,” and as a result, it held that “the
9 ascertainability requirement does not apply to Rule 23(b)(2) actions.” 308 F.R.D. at 597.
10 The court finds the Yahoo court’s reasoning to be persuasive, and adopts it here. The
11 court also notes that Facebook has not cited any cases applying the ascertainability
12 requirement to a (b)(2) class. Thus, to the extent plaintiffs seek certification of a Rule
13 23(b)(2) class, they shall not be required to establish ascertainability.

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

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

1 instances where there was “no URL attachment or object,” Facebook overlooks the fact
2 that plaintiffs’ own class definition specifically carves out these instances:

3 All natural-person Facebook users located within the United States who
4 have sent, or received from a Facebook user, private messages that
5 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
6 the date of the certification of the class.

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

8 By limiting the relevant messages to those “from which Facebook generated a
9 URL attachment,” plaintiffs have already accounted for the supposed outliers discussed
10 in the previous paragraph. Any messages that did not generate a URL attachment (or
11 share object⁴) have already been excluded from the class definition, and thus, they are
12 not relevant to the class certification analysis. Facebook’s arguments would be relevant
13 if plaintiffs had failed to make such an exclusion – but even then, Facebook’s arguments
14 would go more to overbreadth than to ascertainability.

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

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

26
27 ⁴ Facebook’s own opposition brief appears to use the term “URL preview”
28 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”).

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

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

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

20 _____
 21 ⁵ Facebook objects to Dr. Golbeck’s rebuttal report, arguing that it should be stricken.
 22 See Dkt. 169-4. The thrust of Facebook’s objection is that the rebuttal report refers to the
 23 “Titan database,” which was not mentioned in Dr. Golbeck’s opening report. However, it
 24 appears that the rebuttal report simply adds the name of the database, which was
 25 referred to simply as a “database” in the original report. See, e.g., Dkt. 137-6, ¶ 103 (“A
 26 database query could be used”); see also Dkt. 166-6, ¶ 14 (“Although I did not mention
 27 Titan by name in my opening report, I specifically referenced using a database query”).
 28 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

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

17 Facebook also briefly argues that “even if a share object was created, there is
18 more variability” around the way that each share object was handled by Facebook’s
19 system, due to “technical complexities” or other reasons. See Dkt. 178-2 at 13.

20 Facebook’s opposition brief does not develop these arguments, instead directing the
21 court to various parts of the voluminous record filed in connection with the opposition
22 brief. This evidence largely points to situations such as “database failures” or “race
23 conditions” (where multiple people share the same URL at the same time) as creating
24 variabilities, but provides no indication of how often they occur. Indeed, Facebook’s
25 declarant admits that “[a]s with any system of this size, it is expected that at least some
26 machines will always be offline or not functioning properly resulting in some error.” The

27
28 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.

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

6 1. Rule 23(a)

7 a. Numerosity

8 Rule 23(a)(1) requires that a class be so numerous that joinder of all members is
9 impracticable. In order to satisfy this requirement, plaintiffs need not state the “exact”
10 number of potential class members, nor is there a specific number that is required. See
11 In re Rubber Chems. Antitrust Litig., 232 F.R.D. 346, 350-51 (N.D. Cal. 2005). Rather,
12 the specific facts of each case must be examined. In re Beer Distrib. Antitrust Litig., 188
13 F.R.D. 557, 561 (N.D. Cal. 1999) (citing General Tel. Co. v. EEOC, 446 U.S. 318, 330
14 (1980)). While the ultimate issue in evaluating this factor is whether the class is too large
15 to make joinder practicable, courts generally find that the numerosity factor is satisfied if
16 the class comprises 40 or more members, and will find that it has not been satisfied when
17 the class comprises 21 or fewer. See, e.g., Consolidated Rail Corp. v. Town of Hyde
18 Park, 47 F.3d 473, 483 (2d Cir. 1995); Ansari v. New York Univ., 179 F.R.D. 112, 114
19 (S.D.N.Y. 1998).

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

1 b. Commonality

2 Rule 23(a)(2) requires “questions of law or fact common to the class.” This
3 provision requires plaintiffs to “demonstrate that the class members ‘have suffered the
4 same injury,’” not merely violations of “the same provision of law.” Dukes, 564 U.S. at
5 349-50 (internal citation omitted). Accordingly, plaintiffs’ claims “must depend upon a
6 common contention” such that “determination of [their] truth or falsity will resolve an issue
7 that is central to the validity of each one of the claims in one stroke.” Id. “What matters
8 to class certification . . . is not the raising of common ‘questions’ – even in droves – but,
9 rather the capacity of a classwide proceeding to generate common answers apt to drive
10 the resolution of the litigation.” Id. (internal citation omitted).

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

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

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

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

6 c. Typicality

7 The third requirement under Rule 23(a) is that the claims or defenses of the class
8 representatives must be typical of the claims or defenses of the class. Fed. R. Civ. P.
9 23(a)(3). Typicality exists if the named plaintiffs' claims are "reasonably coextensive"
10 with those of absent class members. Staton v. Boeing, 327 F.3d 938, 957 (9th Cir.
11 2003). To be considered typical for purposes of class certification, the named plaintiff
12 need not have suffered an identical wrong. Id. Rather, the class representative must be
13 part of the class and possess the same interest and suffer the same injury as the class
14 members. See Falcon, 457 U.S. at 156.

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

1 commonality and typicality requirements of Rule 23 “tend to merge.” Falcon, 457 U.S. at
2 158 n. 13. The Ninth Circuit interprets the typicality requirement permissively. Hanlon v.
3 Chrysler Corp., 150 F.3d 1011, 1020 (9th Cir. 1998).

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

9 d. Adequacy

10 The fourth requirement under Rule 23(a) is adequacy of representation. The court
11 must find that named plaintiffs’ counsel is adequate, and that named plaintiffs can fairly
12 and adequately protect the interests of the class. To satisfy constitutional due process
13 concerns, unnamed class members must be afforded adequate representation before
14 entry of a judgment which binds them. See Hanlon, 150 F.3d at 1020. Legal adequacy
15 is determined by resolution of two questions: (1) whether named plaintiffs and their
16 counsel have any conflicts with class members; and (2) whether named plaintiffs and
17 their counsel will prosecute the action vigorously on behalf of the class. Id. Generally,
18 representation will be found to be adequate when the attorneys representing the class
19 are qualified and competent, and the class representatives are not disqualified by
20 interests antagonistic to the remainder of the class. Lerwill v. Inflight Motion Pictures,
21 582 F.2d 507, 512 (9th Cir. 1978).

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

26 Facebook argues that neither plaintiffs nor their counsel are adequate for three
27 reasons. First, Facebook argues that this suit “was initiated and is driven by class
28 counsel.” Second, Facebook argues that “plaintiffs’ close relationships with class

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

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

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

25 2. Rule 23(b)

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

1 other available methods for fairly and efficiently adjudicating the controversy.”

2 a. Predominance

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

10 In addition, however, Rule 23(b)(3) requires a more stringent analysis than does
11 Rule 23(a)(2). See Comcast Corp. v. Behrend, 133 S.Ct. 1426, 1432 (2013). Rule
12 23(a)(2) simply requires a “common contention” that is “capable of classwide resolution”
13 and “will resolve an issue that is central to the validity of each one of the claims in one
14 stroke.” Amchem, 521 U.S. at 624; see also Comcast, 133 S.Ct. at 1432; Dukes, 564
15 U.S. at 350. By contrast, to satisfy the Rule 23(b)(3) predominance inquiry, it is not
16 enough to establish that common questions of law or fact exist, as it is under Rule
17 23(a)(2)’s commonality requirement. Indeed, the analysis under Rule 23(b)(3) “presumes
18 that the existence of common issues of fact or law have been established pursuant to
19 Rule 23(a)(2).” Hanlon, 150 F.3d at 1022. Rule 23(b)(3) focuses on the “relationship
20 between the common and individual issues.” Id. Under the predominance inquiry, “there
21 is clear justification for handling the dispute on a representative rather than an individual
22 basis” if “common questions present a significant aspect of the case and they can be
23 resolved for all members of the class in a single adjudication” Id., quoted in Mazza,
24 666 F.3d at 589. An essential part of the predominance test is whether “adjudication of
25 common issues will help achieve judicial economy.” In re Wells Fargo Home Loan Mortg.
26 Overtime Pay Litig., 571 F.3d 953, 958 (9th Cir. 2009) (citations and quotations omitted).

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

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

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

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

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

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

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

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

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

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

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

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

1 4, Ex. 27, 28. And when faced with a “high degree of scrutiny from privacy advocates,”
2 the decision was made to “just remove it.” Dkt. 138-4, Ex. 16.

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

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

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

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

10 While the court finds that individual issues of implied consent do not predominate
11 over common ones, at least as to two of the alleged practices, that finding does not end
12 the predominance analysis under Rule 23(b)(3). The court must also consider whether
13 individual issues surrounding damages predominate over common issues, or in other
14 words, that “damages are capable of measurement on a classwide basis.” See Comcast,
15 133 S.Ct. at 1433.

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

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

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

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

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

24 Turning back to the Social Graph, the key flaw underlying plaintiffs’ expert’s
25 methodology is that it assumes that every message intercepted by Facebook resulted in
26

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

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

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

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

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

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

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

1 disproportionate penalty. To be clear, it is not the size of an aggregate damages award
2 that the court finds disproportionate – the size of an aggregate statutory damages award
3 is not a proper consideration on a class certification motion. Bateman v. American Multi-
4 Cinema, Inc., 623 F.3d 708, 721-23 (9th Cir. 2010). Rather, it is the fact that many
5 individual damages awards would be disproportionate, and sorting out those
6 disproportionate damages awards would require individualized analyses that would
7 predominate over common ones. If there was a basis to find that every class members'
8 statutory damages award would be equally excessive, then the court could follow the
9 scenario set forth by the Ninth Circuit in Bateman and wait until after damages are
10 awarded before deciding whether to reduce the award as unconstitutionally excessive.
11 See id. at 723. However, as mentioned above, the decision about whether or not to
12 reduce an excessive damages award would necessarily involve individual questions
13 about whether each specific class member's award was excessive. For that reason, the
14 court finds that individual issues regarding damages would predominate over common
15 ones, regardless of whether plaintiffs seek statutory damages or damages based on
16 Facebook's profits. Accordingly, plaintiffs' motion for class certification under Rule
17 23(b)(3) is DENIED.

18 b. Superiority

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

21 2. Rule 23(b)(2)

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

1 class may nevertheless be appropriate.” Walters v. Reno, 145 F.3d 1032, 1047 (9th Cir.
2 1998).

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

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

11 The arguments raised by Facebook are very similar to those addressed – and
12 rejected – by the court in Yahoo Mail. 308 F.R.D. at 598-601. Yahoo, like Facebook,
13 argued that the requested injunctive relief was “not ‘indivisible’ because Yahoo would
14 have to determine consent on an individual basis.” Id. at 600. However, the court held
15 that Yahoo “misunderstands the ‘indivisibility’ requirement,” which precludes certification
16 only where “each individual class member would be entitled to a different injunction or
17 declaratory judgment against the defendant.” Id. (citing Dukes, 564 U.S. at 360). The
18 Yahoo court cited the Ninth Circuit’s holding that “the mere fact that a class member’s
19 entitlement to relief might differ from individual to individual did not render the requested
20 injunctive relief improperly divisible.” Id. (citing Rodriguez v. Hayes, 591 F.3d 1105,
21 1125-26 (9th Cir. 2009). Instead, “the fact that the plaintiffs sought relief from a single
22 practice was sufficient to satisfy the indivisibility requirement.” Id. (citing Rodriguez at
23 1125-26). The court also notes that, to the extent that Facebook raises implied consent
24 as an issue requiring individual inquiries, that issue is irrelevant to the Rule 23(b)(2)
25 analysis, which does not ask whether common issues predominate over individual ones.
26 Many of other issues regarding “variabilities” between class members that would be
27 relevant under the (b)(3) analysis (either as part of the predominance requirement or the
28 ascertainability requirement) are irrelevant under the (b)(2) analysis.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

IT IS SO ORDERED.

Dated: May 18, 2016



PHYLLIS J. HAMILTON
United States District Judge