Michael W. Sobol (State Bar No. 194857)
msobol@lchb.com
David T. Rudolph (State Bar No. 233457)
drudolph@lchb.com
Melissa Gardner (State Bar No. 289096)
mgardner@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

Hank Bates (State Bar No. 167688)
hbates@cbplaw.com
Allen Carney
acarney@cbplaw.com
David Slade
dslade@cbplaw.com
CARNEY BATES & PULLIAM, PLLC
11311 Arcade Drive
Little Rock, AR 72212
Telephone: 501.312.8500
Facsimile: 501.312.8505

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MATTHEW CAMPBELL and MICHAEL HURLEY, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

FACEBOOK, INC.,

Defendant.

Case No. C 13-05996 PJH

PLAINTIFFS' MOTION FOR CLASS CERTIFICATION

Date: March 16, 2016
Time: 9:00 a.m.
Judge: Hon. Phyllis J. Hamilton
Place: Courtroom 3, 3rd Floor

NOTICE OF MOTION AND MOTION FOR CLASS CERTIFICATION

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that at 9:00 a.m. on March 16, 2016, or as soon thereafter as the matter may be heard by the above-entitled Court, in the courtroom of the Honorable Phyllis J. Hamilton, 1301 Clay Street, Oakland, CA 94612, Plaintiffs Matthew Campbell and Michael Hurley ("Plaintiffs") will and hereby do move under Federal Rule of Civil Procedure 23(b)(3), or in the alternative, Rule 23(b)(2) for an order certifying 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]

This Motion is based on this Notice of Motion and Motion, the within Memorandum of Points and Authorities, the Declarations of Michael Sobol, Hank Bates, David Rudolph, and Melissa Gardner (including as attached thereto, the Reports of experts Jennifer Golbeck and Fernando Torres), filed in support of the Motion, the Court's files in this action, the arguments of counsel, and any other matter that the Court may properly consider.

.

[1] Excluded from the Class are the following individuals and/or entities: 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.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES
(continued)

Page

STATUTES

RULES

TABLE OF AUTHORITIES
(continued)

Page

TREATISES

OTHER AUTHORITIES

I. INTRODUCTION

The Court should certify for class treatment the Plaintiffs' claims under the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.* ("ECPA") and the California Invasion of Privacy Act, Cal. Penal Code §§ 631 *et seq.* ("CIPA"), on behalf of all persons in the United States who sent a private message containing an Internet link (or URL address) via Defendant Facebook, Inc.'s ("Facebook") electronic messaging service, on the grounds that common proof will establish that Facebook unlawfully intercepts the content of private messages in violation of these laws, without the consent of its users, and monetizes the content of these private messages for its sole benefit.

Facebook's routine business practices, confirmed by its operational computer source code, reveal rampant abuses of its users' privacy, continuing to this day. Every time a user sends a private message with an Internet link, Facebook logs the URL address in user-specific computer code. It also contemporaneously redirects the URL information to other data logs which Facebook uses to assist in determining what advertising, such as "Recommendations" of Internet content, to deliver to other targeted users. The interception of this private message content occurs in the time between composition of the message and it arriving in the recipient's in-box, much of it within the nanoseconds after hitting "send" as it is en route to the recipient. Facebook acquires the content of private messages simultaneously with their transmission using distinct and separate devices, *i.e.*, unique source code that stands independently of the code used to send the message.

Facebook admits that it previously captured URL information in private messages to publicly increase "Like" counts on third-party websites (though it hides behind hyper-technical, and erroneous, defenses to liability). However, Facebook admits to just this sliver of its practices to deflect scrutiny from its more pervasive—*and continuing*—acquisition of private message content which more generally informs its targeted advertising. Facebook's obfuscation has included repeated efforts to define Plaintiffs' case as only relating to the increase in the Like counts (in order to, *e.g.*, impede the proper scope of discovery). However, as the rulings of the Court and Magistrate Judge hold, Plaintiffs' ECPA and CIPA claims concern the acquisition of any and all private message content, and are not limited by any single specific use Facebook

makes of that content. As a result, Plaintiffs have amassed relevant evidence demonstrating that with each private message containing a URL, Facebook creates and logs numerous "objects" and "associations" concerning that URL, including user-specific data logs. Indeed, Facebook's own technicians cannot discern the full extent of Facebook's exploitation of users' private message content, stating that developing "functionality" to identify all the objects and associations created in connection with private messages "would likely be impossible." That conduct alone is sufficient for purposes of establishing violations of ECPA and CIPA. However, Facebook also fueled its targeted advertising platform with the intercepted private message content to provide "recommendations" to Facebook users, to provide analytics to third-party websites and developers, as well as to increment the "Like" social plugin counter. Facebook's surreptitious conduct is essential to its ability to become one of the wealthiest corporations on the planet.

The evidence of Facebook's conduct will undoubtedly be common as to the Plaintiffs and the class members, and will command the focus of the trial of this matter. Plaintiffs' and the class members' unwitting entanglement in Facebook's scheme will likewise be demonstrated through common proof. In its ruling on the Motion to Dismiss, this Court noted that Facebook's self-serving disclosures were insufficient to show users' express consent to interception of their private messages. These self-serving statements also comprise common proof of users' lack of consent. Moreover, unlike other cases where it was found that consent could be implied from attendant circumstances, here no such attendant circumstances exist. To the contrary, there is overwhelming, common evidence that Facebook has actively concealed its practices from public view. Facebook's deliberate efforts to hide its unbounded use of private messages will be shown through common evidence and will defeat Facebook's cynical attempt to imply users' knowing and intelligent relinquishment of their privacy rights.

Class certification under Rule 23(b)(3) is appropriate because the trial of this matter will predominately consist of common evidence establishing Facebook's liability and Plaintiffs' and class members' entitlement to statutory damages or restitution. Alternatively, class certification of Plaintiffs' request for declaratory and injunctive relief is appropriate under Rule 23(b)(2) because Facebook's unlawful interception, scanning and sharing of the content of private

messages, is conduct "generally applicable to the class as a whole."

Accordingly, Plaintiffs request that the Court grant their motion for class certification, appoint plaintiffs as class representatives, and appoint Lieff Cabraser Heimann & Bernstein and Carney Bates & Pulliam as class counsel.

II. ISSUE TO BE DECIDED

Whether plaintiffs' claims satisfy the requirements for class certification under Federal Rule of Civil Procedure 23(a) and 23(b)(3), or in the alternative Rule 23(b)(2).

III. STATEMENT OF FACTS—HOW FACEBOOK ACQUIRES, REDIRECTS AND USES URL CONTENT FROM PRIVATE MESSAGES

Facebook systematically employs computer source code devices, designed for the exclusive purpose of acquiring the content of users' private messages and redirecting it to various data logs, contemporaneously with, but prior to completion of, the transmission of the message to the recipient. The source code Facebook employs to capture and redirect private message content is distinct from, and wholly unnecessary for, the transmission of the message, the scanning of the message for malware or illegal content, or even for generating the thumbnail preview of the URL destination. Facebook's interception of private messages allows its source code to divine the meaning of the messages content and record their characteristics as data points in multiple databases.

After intercepting these records in transit, Facebook retains them indefinitely for future use. Facebook acknowledges one such use— its former practice of bumping up the "Like" count on other websites, which it ceased doing shortly after this practice was publicly exposed in October 2012. Facebook has claimed several times in this litigation that it has changed its business practices, implying that it no longer intercepts the content of private messages.[1]

[1] When this Court asked Facebook's counsel: "[w]hen you say 'the cessation of conduct,' what specific conduct ceased?" Ex. 1 (October 1, 2015 Hearing Transcript at 5:10-11), Facebook's counsel only identified the increment in the Like counter. *Id.* at 7:4-7 ("If you included the URL in the message, this anonymous aggregate number…went up, and that's the conduct, that's – that stopped"). The Court pressed, asking, "[b]ut did the actual conduct of scanning or looking at these messages that are sent stop?" *Id.* at 8:9-10. Facebook's counsel did not respond directly, but rather began discussing scanning for purposes of detecting malware or criminal conduct, but nothing else. *Id.* at 9:2-9.

However, Facebook's source code not only reveals that Facebook *continues* to acquire URL content from private messages, but that it also continues to make use of the content it acquires.

A. Facebook Intercepts Content From Private Messages During Transmission

As alleged in the Consolidated Amended Complaint ("CAC") and detailed in the Report of Dr. Jennifer Golbeck in Support of Plaintiffs' Motion for Class Certification ("Golbeck Report"), Facebook "intercepts" private messages while in transit, using source code-based devices designed solely for the purpose of exploiting their content.[2]

Facebook employs a component of its source code to scan private messages, while they are being composed, to detect the presence of a URL.[3] Once a URL has been detected, a request is sent to Facebook's servers to retrieve information related to the URL. If no information related to the URL is contained on Facebook's server, Facebook "scrapes" the website associated with the URL to retrieve various types of information. One of the purposes of retrieving this information is to create a URL attachment and "preview," which Facebook describes as "a brief description of the URL and, if available, a relevant image from the website."[4]

Thereafter, employing a separate and distinct component of its source code, when the user presses "send," Facebook detects whether the message contains a URL attachment and, if so, processes data in the message in order to create a record of the fact that the user sent the specific URL.[5] This record, called an "EntShare," uniquely identifies the user by her Facebook ID ("FBID") and uniquely identifies the URL from her message.[6] Additionally, Facebook creates an association between the EntShare record—which ties the individual user to the URL—and a record called a "EntGlobalShare," which Facebook uses to track activity among all of its users relating to a particular URL.[7]

---

[2] Ex. 2 (Golbeck Report) at ¶¶ 32-55; 116-118. Unless otherwise stated, all exhibits are to the Declaration of Melissa Gardner in Support of Plaintiffs' Motion for Class Certification.

[3] *Id.* at ¶¶ 19-29.

[4] Ex. 3 (Facebook's Suppl. Responses and Objections to Plaintiffs' First Set of Interrogatories), at 13:4-5.

[5] Ex. 2 (Golbeck Report), at ¶¶ 40-42.

[6] *Id.* at ¶ 100.

[7] *Id.* at ¶ 41.

Facebook code further intercepts and redirects private message content by extracting, then logging, URL data from private messages in various tables that Facebook uses to target content to other users.[8] For example, in one instance, private message content is sent to, and logged in, the "share_stats" table. Facebook exploits the data in the share_stats table in a variety of ways, including making recommendations of Internet content other users, particularly if a Facebook "friend" has contributed to the relevant share_stats count.[9] In another instance, Facebook logs URLs being shared in private messages in its "Nectar" platform, which makes that data available to developers through Facebook's "Insights" product, described below.[10]

In sum, Facebook employs unique code-based devices to intercept, redirect and log the contents of user's private messages, including code that creates the data points represented in EntShare objects, a code that logs the content of user's private messages for use by Facebook, and a code that incremented the "Like" counter on third-party websites.[11] This content interception happens in the initial stages of the private message's transmission, before any part of the message is in storage.[12] Facebook did not need to create these data points to process or send the message, and Facebook employs separate and distinct code to direct the private message from the sender to the recipient's inbox.[13]

The above-described transmission procedures and code, including the code pertaining to the interception of message content and creation of EntShare and EntGlobalShare records, has remained consistent from the beginning of the class period to the present.[14]

---

[8] *Id.* at ¶¶ 43-54.

[9] *Id.* at ¶¶ 44-51; 57-64.

[10] *Id.* at ¶ 41.

[11] *Id.* at ¶ 55.

[12] *Id.* at ¶¶ 108-115;117.

[13] *Id.* at ¶¶ 19-29; 108-115.

[14] *Id.* at ¶ 107. The most current version of the Facebook source code that Facebook has produced is dated December 31, 2012, and while the descriptions of the source code set forth herein are as of that date, Facebook has not produced, or informed Plaintiffs of, any material and relevant changes to Facebook's source code since then, if any. Notably, Facebook's production of documents show that as of at least April 20, 2104, Facebook was detecting URL content in the named Plaintiffs' private messages and created EntShare-related objects therefrom. *Id.* at ¶ 96; Ex. 35 (FB000005802-R).

B. Facebook Uses Content From Intercepted Private Messages

According to Facebook, the extent of the records it creates from private message content border on limitless, as do the uses to which it puts such content. In a declaration in this proceeding, a Facebook Engineering Manager acknowledged: "Neither I, nor any other person to my knowledge, is aware of all possible Objects that could be created in connection with processing a Facebook message" [15] and that "ascertain[ing] the identity of every Object or Association that could possibly be generated from a message, [would] require consulting with engineers in every group who have worked on every past or present product or feature at Facebook." [16] Turning to how Facebook uses the intercepted content, the same declarant explained the possibilities are as expansive as Facebook's entire source code: "the comprehensive record of Facebook functions that used any given Object or Association type at any given time is Facebook's source code." [17] Accordingly, "the abstract hypothetical question as to all possible uses is likely impossible to answer."[18]

Facebook places no limitations on how it may exploit its users' data, including the data it acquires from its users' private messages. Facebook has large and complex data behind its site. Facebook currently stores this data in a data model called TAO (The Associations and Objects).[19] Objects represent *things* on Facebook—*e.g.*, users, pages, checkins, comments, locations. Associations represent *relationships* between objects—*e.g.*, friendships between users, a Like that connects a user to a page, or a location that is tied to a user check-in.[20] In deposition, Facebook's 30(b)(6) witness testifying on how the company uses private message content stated that "*any engineer can build a system to add any associations between any objects*."[21] Thus, the records that Facebook creates from its users' private messages, and which are stored indefinitely, may be put to any use, for any reason, by any Facebook employee, at any time.

---

[15] Declaration of Dale Harrison for Defendant Facebook, Inc. (Dkt No. 125, Ex. A), at ¶ 17.
[16] *Id.* at ¶ 19.
[17] *Id.* at 20.
[18] *Id.*
[19] Ex. 2 (Golbeck Report), at ¶ 32.
[20] *Id.* at ¶ 33.
[21] Ex. 5 (September 25, 2015 Deposition of Ray He, "He Dep."), at 172:2-3.

1. Facebook Uses Records Created From Private Message Interceptions to Fuel Its Algorithms for Measuring User Engagement and Making Recommendations

Facebook's code is written to scan private messages and extract the number of times a URL is shared in private messages. Specifically, during the creation of the EntShare, an association is created between the EntShare and its related EntGlobalShare. Each EntGlobalShare contains a field titled "tracking info," which contains a string of five numbers, separated by commas (a "comma-delimited string").[22] Respectively, those numbers represent the total number of (1) shares ("share_count"), (2) posts ("post_count"), (3) Likes ("like_count"), (4) comments ("comment_count"), and (5) clicks ("click_count").[23] When an EntShare is created, Facebook's code creates an association between that EntShare (tying the user and the URL together) and the EntGlobalShare (recording the entirety of Facebook user activity in relation to the URL).[24] In other words, Facebook's code is written so that the number of EntShares created from private message content will equal the "share_count" in the corresponding EntGlobalShare.

The tally of the number of times a URL was discussed in private messages—*i.e.*, the number reflected in the "share_count" value in the "tracking_info" field of an EntGlobalShare—was and continues to be used by Facebook for purposes beyond simply increasing the publicly displayed "Like" count on the website associated with that URL, conduct to which Facebook has already publicly admitted. During the class period, Facebook also used the share_count value to determine a URL's popularity among Facebook users and further incorporated *that* information into secret algorithms that pushed content to users across the social network.[25]

As one example, Facebook utilized a system called "Taste" to generate

---

[22] *See, e.g.*, Ex. 4 (FB000005502-R) (in which the field designated "tracking_info" contains the string "12,10,2,19,0").

[23] Ex. 6 (FB000008489) at 2 ("tracking_info contains these numbers in a comma delimited string…share_count, post_count, like_count, comment_count, click_count"); *See also* Golbeck Decl. ¶ 38 ("The EntGlobalShare also contains a number of tracking information fields, including 'share_count,' 'post_count,' 'like_count,' 'comment_count,' and 'click_count.'")

[24] This is achieved through a series of calls within the code, culminating in the command "ShareURLTracking::updateUrlCounts(…)" in which the "share_count" value in the "tracking_info" field of the EntGlobalShare is incremented by 1. Ex. 2 (Golbeck Report), at ¶ 84.

[25] *Id.* at ¶¶ 56-64.

"recommendations," or links to recommended websites, to push to targeted users that Facebook believes the user would find relevant, both on Facebook and on third-party websites.[26] Taste utilizes the share_count information obtained from user's private messages to generate recommended links for users.[27] These "recommendations" were targeted to specific users based upon, among other things, what their friends shared on Facebook. Prior to implementing Taste, Facebook implemented a source code device known as "ExternalNodeRecommender" to generate a list of recommended websites for users using the share_count information extracted from user's private messages.[28] The ExternalNodeRecommender also took into account what URLs a user's friends had shared in order recommend specific websites to users.[29] Thus, Facebook's recommendation system used private message content to target Internet links to specific users.

2. Facebook's Sharing of User Data With Third Parties.

Facebook intentionally and publicly shared demographic data about its users and their private messages with website owners and developers.[30] Facebook employed multiple source-code devices to redirect the contents of private messages to these interested third parties. Facebook's "Insights" product, directed to website owners, provides demographic information about interactions on external websites. This includes data obtained from interceptions of URL content in private messages, including demographic information about the message's sender. Facebook makes this information available to any website owner, with the pitch that such information will help the website customize content for its existing visitors and target advertising (presumably, via Facebook) to attract new visitors. Additionally, Facebook's API ("application program interface") allowed third-party app developers to query the number of times a URL was shared on Facebook, which number included the number of times that URL was sent via a private message. This content could be used for any purpose and by any developer.

[26] Facebook documents describe Taste as "recommendation systems for discovery." Ex. 7 (FB000003118). Ray He further explains that "Taste is a back end for providing recommendations" and that "[a] recommendation is a link, typically, a link that we think a user would find relevant." Ex. 5 (He Dep.) at 227:3-4; 11-12.

[27] Ex. 5 (He Dep.), at 229:19-230:6.

[28] Ex. 2 (Golbeck Report), at ¶¶ 61-64.

[29] *Id.*

[30] Ex. 33 (Torres Report), at ¶ 16.

3. Increasing "Like" Counts on Third-Party Websites

The Like button is critical for Facebook's targeted advertising business.[31] The Like button allows Facebook to monitor its users' activity, even when those users are on third-party websites.[32] With active Likes, if a user clicks a "Like," Facebook ties that data point to the user and, if the third-party website has applied certain metadata to the URL associated with the Like button, Facebook registers the Like as a data point in its marketing profile, enabling both Facebook[33] *and* the website[34] to target the user with ads and messages. Further, through Facebook's Insights product, the Like button enables a third-party website to covertly monitor Facebook users' interaction with the website—Facebook promotes this feature as helping the website "tailor your content and products to your users" by providing "demographic information for the interactions that occur on your site and on Facebook."[35]

Prior to October 2012, Facebook used the combined values in the "tracking_info" field of an EntGlobalShare—including the share_count derived from private message content—as the Like count publicly displayed on the corresponding third-party website.[36] However, when exposed by the Wall Street Journal in early October 2012, Facebook conducted a cost/benefit analysis and decided to quickly and quietly abandon the *public-facing portion* of this practice.[37]

---

[31] *See, e.g.*, Ex. 8 (FB000014365), a 2012 email in which a Facebook employee states "It is an acknowledged problem that a shortage of likes is limiting the number of users that can be targeted by their interests and thereby affecting revenue." When explaining what data contributes to the Like count (including URLs found through private message scans), Facebook employee Austin Haugen states "the motivation was to make [the Like count] as big as possible." Ex. 9 (FB000003335). *See also* Ex. 10 (FB000004996) ("we don't want to dilute our count—we want to have the biggest count.")

[32] *See, e.g.*, Ex. 11 (FB000012539), at 2: "[W]hen a user establishes a connection by clicking Like on one of your Open Graph-enabled pages, you gain all lasting capabilities of Facebook Pages: a link from the user's profile, ability to publish to the user's News Feed, inclusion in search on Facebook and analytics through our new Insights product. In summary, by giving your users better, simpler ways to connect with the content on your service, you can then use those connections to provide more personalized, relevant experiences."

[33] *See, e.g.*, Ex. 12 (FB000008268), a Facebook document entitled "Targeting criteria organized into 5 groups," which includes the group marked "Interests," later clarified to mean "[t]argeting based on user interests, determined by [among other things] Likes."

[34] Facebook does this through its Open Graph Protocol, a portion of its platform dedicated to linking items of data across its social network. *See, e.g.*, Ex. 11 (FB000012539) at 2.

[35] Ex. 13 (FB000008722), at 2.

[36] Ex. 2 (Golbeck Report), at ¶¶ 82-93.

[37] For example, a Facebook code edit from this period, titled "URL Tracking Adjustments," states

Footnote continued on next page

Indeed, the value of Likes to the business was recognized at the highest levels of the company.[38] In an October 16, 2012 code fix titled "Remove Private messages from Like Button Count" Facebook engineer [redacted] notes that "[t]hese [private message scans] were contributing 0.8-4% of the count depending on domain. Given the low contribution and high degree of scrutiny from privacy advocates, let's just remove it."[39] In the same document, [redacted] further comments that this is a "[p]ress issue—need to push asap." *Id*. However, Facebook took pains to hide this practice from the public.[40]

Nonetheless, Facebook continues to create EntShares from private messages containing URLs, and additionally continues to increment the "share_count" value within corresponding EntGlobalShares.[41] As discussed above, Facebook uses that data in a variety of ways, each of which ultimately allows Facebook to profit from private messages.

In short, Facebook has intercepted users' private message content has used it for profit, and appears to be doing so to this day.

IV. CLASS CERTIFICATION IS PROPER

Certification of the following class is proper under Fed. R. Civ. P. 23:

> 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

Footnote continued from previous page
"The purpose of this change is to be able to accurately determine what % of the like counts are attributable to private messages. If the % is low enough, we will cut this tracking due to privacy concerns." Ex. 14 (FB000000594).

[38] In a September 2012 email exchange between Facebook [redacted] and engineer [redacted] complained that "more and more I'm seeing Twitter's [social plugin] numbers be much greater than ours. Either their traffic has grown significantly, their spam has grown significantly or they're counting something different than we are. Regardless, big numbers are good, so it seems like we should be showing the largest number we can rationalize showing." Ex. 15 (FB000008304). [redacted] responded that they had been including "shares on fb [including URLs in private messages] for two years now and started doing so in response to Twitter's reported numbers." *Id.*

[39] Ex. 16 (FB000001265).

[40] When engineers discussed the inclusion of metrics such as private message scans in the publicly displayed "Like" count on website, they noted "[w]e have intentionally not proactively messaged what this number is since it's kind of sketchy how we construct it." Ex. 17 (FB000006429) at 3.

[41] Ex. 2 (Golbeck Report), at ¶¶ 90-92.

class.[42]

Without certification of an appropriate class, privacy rights long acknowledged in the Common Law, as reflected in the legislative enactments of ECPA and CIPA, will go unenforced, thus eviscerating the privacy interests necessary to the sound functioning of a democratic society. *See, e.g.*, J. Cohen, *What Privacy Is For*, 126 Harv. L. Rev. 1904, 1927 (2013) ("In addition, privacy does not only protect individuals. Privacy furthers fundamental public policy goals relating to liberal democratic citizenship, innovation, and human flourishing.").

A. The Rule 23(a) Criteria Are Met

Plaintiffs have set forth *prima facie* facts that satisfy the four requirements of Rule 23(a): (1) numerosity; (2) commonality; (3) typicality; and (4) adequacy of representation.

1. The Class is so Numerous that Joinder is Impracticable

Plaintiffs satisfy the numerosity requirement because the class "is so numerous that joinder of all members is impracticable." Fed. R. Civ. P. 23(a)(1). "Where 'the exact size of the class is unknown, but general knowledge and common sense indicate that it is large, the numerosity requirement is satisfied.'" *In re Abbott Labs. Norvir Antitrust Litig.*, Nos. 04–1511, 04–4203, 2007 WL 1689899, at *6 (N.D. Cal. June 11, 2007) (Wilken, J.) (quoting *Newberg on Class Actions* § 3.3 (4th ed. 2002)). During 2012, Facebook identified approximately 600 million monthly active users who utilized the private message function.[43] Facebook's Q4 earnings statement from 2012 states that it had 1.056 billion monthly active users worldwide, with

[42] Excluded from the Class are the following individuals and/or entities: 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.

[43] In Ex. 18 (FB000008271), at 4, Facebook employee [redacted] identifies the "active user account for messages" via an internal Facebook report at "~600M MAUs." In this instance "MAU" appears to stand for "Monthly Active User," a term Facebook uses elsewhere in the course of describing user engagement. *See, e.g.*, Facebook's press release for Second Quarter 2015 financial results (defining "MAUs" as "[m]onthly active users.") (available at http://investor.fb.com/releasedetail.cfm?ReleaseID=924562).

193 million of those users located in North America.[44] Assuming an even distribution among active message users worldwide, this means as many as tens of millions of members exist in the United States, such that even a tiny percentage of those users would satisfy the numerosity requirement.

2. Questions of Law and Fact Are Common to the Class

Rule 23(a)(2) requires that there be "questions of law or fact common to the class." Commonality is thus satisfied where the claims of all class members "depend upon a common contention...of such a nature that it is capable of classwide resolution—which means that determination of its truth or falsity will resolve an issue that is central to the validity of each one of the claims in one stroke." *Wal-Mart Stores, Inc. v. Dukes*, 131 S. Ct. 2541, 2551 (2011) (common questions must "generate common answers" that are "apt to drive the resolution of the litigation") (citation omitted). "All questions of fact and law need not be common to satisfy the rule." *Hanlon v. Chrysler Corp*., 150 F.3d 1011, 1019 (9th Cir. 1998); *Rodriguez v. Hayes*, 591 F.3d 1105, 1122 (9th Cir. 2010) (noting that "common" does not mean "complete congruence"). In fact, "[t]hat 'commonality only requires a single significant question of law or fact' was recently recognized by both the Supreme Court and the Ninth Circuit." *Vietnam Veterans of Am. v. C.I.A.*, 288 F.R.D. 192, 212-13 (N.D. Cal. 2012) (Wilken, J.) (citations omitted) (citing cases).

In the Joint Case Management Conference Statement, Facebook itself identifies relevant common issues which track the elements to establish Facebook's violations of ECPA and CIPA. *See* Dkt. 6 at 4-7.[45] Proof of the elements of ECPA and CIPA is necessarily common because it will focus upon Facebook's uniform conduct. Such evidence will concern Facebook's internal operations and source code, revealing its "intent," to "intercept" private messages while in transit, deriving its "content" and "redirecting" it elsewhere for purposes outside the "ordinary course of

[44] Ex. 19 (Facebook Quarterly Earnings Slides Q4 2012) at 3.

[45] Common questions identified by Facebook include: (a) whether Facebook unlawfully 'redirected' the content of users' private messages; (b) whether the interception was contemporaneous with the messages' transmission; (c) whether the "ordinary course of business" exemption applies to Facebook's conduct; and (d) whether Plaintiffs and the class members expressly or impliedly consented to the interceptions. *Id*.

its business." Here, even the issue of Plaintiffs' lack of consent to Facebook's conduct will focus on Facebook's conduct, *i.e.*, its failure to procure express consent, and its secret, but active concealment of its actual practices. Therefore, proof of these elements will necessarily require the same evidence for any one Plaintiff as it will for the class as a whole, and resolution of these issues will necessarily generate common answers.

3. Plaintiffs' Claims Are Typical of the Class

Rule 23(a)(3)'s "typicality requirement is to assure that the interest of the named representative aligns with the interests of the class." *Wolin v. Jaguar Land Rover North America*, 617 F.3d 1168, 1175 (9th Cir. 2010) (quoting *Hanon v. Dataproducts Corp.*, 976 F.2d 497, 508 (9th Cir. 1992)). Typicality exists when the class representatives and the class members are subjected to and injured by the same course of conduct. *Ellis v. Costco Wholesale Corp.*, 657 F.3d 970, 984 (9th Cir. 2011).

Representative Plaintiffs Matthew Campbell and Michael Hurley are Facebook users who have sent private messages which contained a URL, or Internet link.[46] Discovery in this case has confirmed that by operation of its source code and internal policies, Facebook intercepted the representative Plaintiffs' private messages, acquired the messages' content, redirected those messages to generate records about the content acquired therein, and stored these records, in perpetuity. Ex. 20 (Defs.' Suppl. Resp. and Objs. To Narrowed Second Set of Interrogatories), at Ex. 1. Discovery has further revealed that Facebook processed and scanned all private messages on the same technological platform, and that Facebook's code, and accompanying, code-based message-scanning devices, operated uniformly across all class members.[47] Any Facebook user in the class sending a private message would have URL content intercepted in the same manner as the representative Plaintiffs. Accordingly, the representative Plaintiffs' claims and the class members' claims "are so interrelated that the interests of the class members will be fairly and adequately protected in their absence." *Gen. Tel. Co. of Sw. v. Falcon*, 457 U.S. 147, 163 n.13 (1982); *Ades v. Omni Hotels Mgmt. Corp.*, No. 13-02468, 2014 WL 4627271, at *9 (C.D. Cal.

[46] *Id.*

[47] Ex. 2 (Golbeck Report), at ¶ 107.

Sept. 8, 2014) (finding class representatives' claims typical where "course of conduct…common to the class, and privacy invasions typical to those of the class generally" were alleged).

4. Plaintiffs And their Counsel Will Adequately Represent the Class

Rule 23(a)(4) requires that the class representatives and their counsel will "fairly and adequately protect the interests of the class." *See Ellis*, 657 F.3d at 985 (quoting *Hanlon*, 150 F.3d at 1020). "Adequate representation depends on, among other factors, an absence of antagonism between representatives and absentees, and a sharing of interest between representatives and absentees." *Id*. In considering the adequacy of plaintiffs' counsel, the court must consider "(i) the work counsel has done in identifying or investigating potential claims in the action; (ii) counsel's experience in handling class actions, other complex litigation, and the types of claims asserted in the action; (iii) counsel's knowledge of the applicable law; and (iv) the resources that counsel will commit to representing the class." Fed. R. Civ. P. 23(g)(1)(A).

As Plaintiffs' claims are typical of the class, they have no antagonism with class members' interests. Plaintiffs also have committed to prosecute the case vigorously on behalf of all class members, and have devoted substantial time and effort in the case already. Plaintiffs have retained counsel with substantial experience in litigating privacy claims and class actions generally. Bates Decl. Ex. A; Sobol Decl. ¶ 5. Plaintiffs' counsel have devoted a significant amount of time to identifying and investigating the potential claims and pursuing discovery in this matter, and will continue to commit the resources necessary to represent the class. Accordingly, Plaintiffs and their counsel will adequately represent the class.

5. The Class Is Ascertainable

"[C]ourts have implied an additional requirement under Rule 23(a): that the class to be certified be ascertainable." *In re Google Inc. Gmail Litig.*, No. 13-02430, 2014 WL 1102660, at *10 (N.D. Cal. Mar. 18, 2014) (Koh, J.). "'A class definition should be precise, objective, and presently ascertainable,' though 'the class need not be so ascertainable that every potential member can be identified at the commencement of the action.'" *Gray v. Golden Gate Nat'l Recreational Area*, 279 F.R.D. 501, 508 (N.D. Cal. 2011) (LaPorte, J.) (quoting *O'Connor v. Boeing N. Am., Inc.*, 184 F.R.D. 311, 319 (C.D. Cal. 1998)). "A class definition is sufficient if

the description of the class is 'definite enough so that it is administratively feasible for a court to ascertain whether an individual is a member.'" *In re High-Tech Employee Antitrust Litig*., 985 F. Supp. 2d 1167, 1182 (N.D. Cal. 2013) (Koh, J.) (quoting *O'Connor*, 184 F.R.D. at 319). It must be possible to determine whether a class member is included "by reference to objective criteria." *Id*. (quoting 5 James W. Moore, *Moore's Federal Practice*, § 23.21[3] (Matthew Bender 3d ed.)).

Plaintiffs have precisely defined the class based on objective criteria.[48] Dr. Golbeck has demonstrated that, by running some simple lines of code, Facebook can identify all Facebook users in the United States during the relevant time period from whose messages Facebook has intercepted URL content and retained that content in its EntShare database. [49] In any event, any Facebook user can readily determine whether she sent or received a Facebook message containing a URL within the relevant time period.

B. The Class Is Properly Maintained Under Fed. R. Civ. P. 23(b)(3)

Rule 23(b)(3) permits the maintenance of a class where common issues predominate and a class action is superior to individual actions.

1. Common Issues Predominate

The predominance requirement "tests whether proposed classes are sufficiently cohesive to warrant adjudication by representation." *Amchem Prods., Inc. v. Windsor*, 521 U.S. 591, 623 (1997). Predominance is satisfied when "[a] common nucleus of facts and potential legal remedies dominate [the] litigation." *Hanlon*, 150 F.3d at 1022. "When common questions present a significant aspect of the case and they can be resolved for all members of the class in a single adjudication, there is clear justification for handling the dispute on a representative rather

[48] "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). . . ." When a user includes a URL in a private message, Facebook's source code detects the URL and generates an attachment to the message. Ex. 2 (Golbeck Report), at ¶¶ 18-29. While the private message is still in transit, the source code captures the content private messages embodied in the URL attachment, redirecting it to various data logs or databases to target advertising. *Id*. at ¶¶ 30-54. Facebook has nit-picked elsewhere that not every URL embedded in a private message gets detected. Although this is the rare exception, Plaintiffs have tailored the class definition by referring to the generation of the URL attachment because, by operation of Facebook's source code, every URL attachment is detected.

[49] *Id.* at ¶¶ 98-106. In the EntShare database, private message URL content is stored, linked with a user specific identification.

than on an individual basis." *Hanlon*, 150 F.3d at 1022. (citation omitted).

This case turns on evidence of Facebook's uniform treatment of millions of class members. Facebook literally programmed itself to operate exactly the same way with regard to all of its users. Common issues of fact and law predominate because 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.

a. Facebook's ECPA Violation Will be Established by Common Proof

Plaintiffs' ECPA claim can be adjudicated based upon evidence common to the class. ECPA provides for civil penalties against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication through the use of any electronic, mechanical, or other device" while in transit. 18 U.S.C. § 2511(1)(a). An "interception" means acquiring the content of the communication such that "the contents of a wire communication are captured or redirected in any way." Order on Motion to Dismiss, Dkt. 43 at 5.

An ECPA claim is naturally suited to classwide determination. In a similar case earlier this year, another court within this District held that "[w]hether Yahoo intercepts emails to and from non-Yahoo mail subscribers while those emails are in transit is 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.'" *In re Yahoo Mail Litig.*, 308 F.R.D. 577, 590-91 (N.D. Cal. 2015) (Koh, J.), *quoting Dukes*, 131 S.Ct. at 2552. Although the court in *Yahoo Mail Litig.* did not reach the issue of predominance because plaintiffs there only sought certification under Fed. R. Civ. P. 23(b)(2), its rationale that these basic elements of an ECPA claim are "central to the validity" of the claims and can be adjudicated classwide, compels a determination of predominance here.

While Facebook denies that it intentionally intercepts private messages while in transit, within the meaning of ECPA, the determination of those issues are undeniably common and

susceptible to common proof. Here, expert analysis of Facebook's source code, corroborated by other internal records, will show that an intentional interception of URL content occurs during transmission and prior to delivery of the private message to the recipient.[50] Moreover, the source code analysis demonstrates that upon interception of private message URL content, Facebook redirected the content to multiple data logs and repositories, such as EntShares and EntGlobalShares, to make use of the content for purposes wholly unrelated to facilitating the transmission of the message.[51]

ECPA has an exception to liability for interceptions conducted through a device that is "being used by a provider of wire or electronic communication service in the ordinary course of its business." 18 U.S.C. § 2510(5)(a); Order on Motion to Dismiss, Dkt. 43 at 6. The determination of Facebook's defense through this exception also will be subject to common proof as it focuses exclusively on Facebook's conduct, source code and development of the private message function. For example, Plaintiffs have determined that Facebook's source code that redirects private message content operates independently of, and at another point in time from, other source code that detects spam, malware, and criminal activity that Facebook asserts is part of the message transmission process.[52] *See* Order on Motion to Dismiss, Dkt. 43 at 12 ("The fact that Facebook can configure its code to scan message content for certain purposes, but not for others, leaves open the possibility that the challenged practice constitutes a separate 'interception.' Simply put, the application of the 'ordinary course of business' exception to this case depends upon the details of Facebook's software code.").

b. Facebook's CIPA Violation Will be Established by Common Proof

As Facebook acknowledges, the core issues in dispute under the CIPA claim mirror the

[50] Ex. 2 (Golbeck Report), at ¶¶ 116-118.

[51] *Id.* at ¶¶ 32-54; 109 ("…use of URL shares in private messages is not necessary for the functionality of message sharing in Facebook.").

[52] *Id.* at ¶¶ 108-115; 55 ("…discrete components of Facebook's source code that execute the interceptions, each of which operate as separate devices, *i.e.*, they each perform separate and unique functions, and their deletion from the code would still leave intact the functioning of the other devices used to process and deliver the messages.").

issues applicable to the ECPA claim. Dkt. 60 at 7. For the reasons set forth above, common issues clearly predominate.

At the class certification stage, this Court must ensure that a nationwide class under the law of a single state, CIPA, comports with due process. *Phillips Petroleum Co. v. Shutts*, 472 U.S. 797, 818 (1985). California's choice of law rules govern this consideration. *Klaxon Co. v. Stentor Elec. Mfg. Co.*, 313 U.S. 487, 496 (1941); *Zinser v. Accufix Research Inst., Inc*., 253 F.3d 1180, 1187 (9th Cir. 2001). The starting point in this analysis is Facebook's terms of service, which provide that "the laws of the State of California will govern…any claim that might arise between you and us."[53] *See Nedlloyd Lines B.V. v. Super. Ct*., 3 Cal. 4th 459, 468-70 (1992) (concluding that where the parties have entered into an agreement that specifies that a particular jurisdiction's law will govern their disputes, a court's choice-of-law analysis should begin with an inquiry into whether the claims of putative class members fall within its scope). The broad scope of Facebook's choice-of-law provision clearly evidences an intent to have California law apply to all disputes arising out of the relationship between Facebook and its users. Moreover, California law has a substantial relationship to the parties. *Nedlloyd*, 3 Cal. 4th at 464. A substantial relationship exists where one of the parties has its principal place of business in the chosen state. *ABF Capital Corp. v. Osley*, 414 F.3d 1061, 1065 (9th Cir. 2005). Accordingly, certification of a CIPA claim on behalf of a nationwide class is appropriate. *See Wolph v. Acer Am. Corp*., 272 F.R.D. 477, 484-85 (N.D. Cal. 2011) (White, J.).

c. Plaintiffs' and the Class Members' Lack of Consent to Facebook Practices will be Established Through Common Proof

Both ECPA and CIPA require that the offending interception occur without the consent of the user. In the ruling on the Motion to Dismiss, the Court reviewed all of Facebook's relevant disclosures and concluded: "…in the context of express consent, any consent with respect to the processing and sending of messages itself does not necessarily constitute consent to the specific practice alleged in this case—that is, the scanning of message content for use in targeted advertising." Order on Motion to Dismiss, Dkt. 43 at 16. The three iterations of Facebook's Data

[53] Ex. 21 (FB000000001), at 7; Ex. 22 (FB000000032), at 8; Ex. 23 (FB000000058), at 6.

Use Policy during the class period were applicable to all class members and therefore constitute common proof, making the issue of whether these terms disclosed Facebook's practices of scanning private messages suitable for a classwide determination. Exs. 24 – 26. *Gmail*, 2014 WL 1102660, at *15 (finding that express consent is a common question for class members exposed to the same disclosures).

In critical respects, this case is not like *Gmail*, where the Court found that individual issues regarding actual, *implied* consent would predominate. There, the record was replete with evidence of class members' potential, actual advance notice of Google's practices making implied consent "an intensely individualized" factual question. *Id.* at *20. Here, in contrast, there is a complete absence of any evidence of advance notice. Despite extensive discovery, including not only the depositions of the class representatives, but also the depositions of the recipients of the class representatives' private messages, Facebook has not produced relevant evidence from which actual notice can be reasonably implied. *Silbaugh v. Viking Mag. Servs.*, 278 F.R.D. 389, 393 (N.D. Ill. 2012) ("Having produced no evidence that any individual consented to receive the text messages…defendant is unable to realistically argue that individual issues regarding consent outweigh the commonality.") Thus, unlike *Gmail*, there is no indication that individual consent issues will overwhelm issues Plaintiffs have shown herein to be resolvable through classwide proof.

Rather, this case is more like *Omni Hotels*, where the court found predominance in the absence of actual notification to the class members. 2014 WL 4627271, at 13. Here, Facebook's undisclosed use of private message content was so extensive that actual consent to the scope of its practices is not reasonably possible. Facebook's 30(b)(6) witness testified on the topic of Facebook's use of private message content, stating that "any engineer can build a system to add any associations between any objects." Ex. 5 (He Dep.) at 172:1-3. Thus, the records that Facebook creates from its users' private messages, and which are stored indefinitely, have no limitation, and may be put to any use, for any reason, by any Facebook employee, at any point in the future. Facebook's Engineering Manager submitted a declaration asserting that not even Facebook can determine the extent to which it uses private message content, and that finding a

way to identify all objects created in connection with a given Facebook message, "would likely be impossible." Dkt. 126 (Harrison Decl.), at ¶ 12. If Facebook cannot identify the extent of its use of private message content, surely the average user cannot be implied to have that actual knowledge of those practices.

Further, Plaintiffs will present common evidence that rather than disclose its practices (to provide some basis for "actual" knowledge necessary to imply consent), Facebook actively sought to conceal its practices from users. In fact, whether Facebook's cover-up of its actions defeats any findings of implied consent here, will be a common question. *Gmail*, 2014 WL 1102660, at *14 (noting that disclosures by Google which indicated that scanning was *not* occurring indicated "the opposite" of establishing consent). Throughout the class period, and afterwards, Facebook has known that its users were *not* aware of the scanning at issue in this case, and has affirmatively tried to prevent them from finding out. *See, e.g.* Ex. 27 (FB000006435), at 3-6 ("We have intentionally not proactively messaged what [the Like] number is since its kind of sketchy how we construct it." … "if we say '2,304 people like this,' but only 1,300 people like this, it's just downright misleading. I think we should just swallow this bullet and make the Like button map to the number of people who like this thing."); *See also* Ex. 28 (FB000004406) ("Whether it is written in the small print of the platform on not, the understanding of 99.9% of people is that like is an explicit action [distinct from including a URL in a private message]…I fear that we will get dashed against the rocks in Europe for this.") Indeed, with regard to Facebook's incrementing of the Like counter, its executives determined that they "should report this as fixing an accounting error rather than describing exactly what happened because it was a privacy issue letting the count be that high." Ex. 29 (FB000007924), at 2. Indeed, when reversing that practice, Facebook kept it deliberately quiet. *See* Ex. 30 (FB000000502) ("[G]iven the low contribution [to the overall Like count on third party websites] and high degree of scrutiny from privacy advocates, let's just remove it.")

Discovery also demonstrates that Facebook's public-facing statements about "procedural safeguards" for ensuring user privacy in product development are false. Facebook has represented, *inter alia*, in its filings with the Security and Exchange Commission that it has "a

dedicated team of privacy professionals who are involved in new product and feature development from design through launch" and who conduct "ongoing review and monitoring of the way data is handled by existing features and applications."[54] However, when asked to produce documents sufficient to identify the individuals comprising this "dedicated team,"[55] Facebook responded that *none* existed.[56]

d. Allocation of Monetary Relief to Plaintiffs and the Class can be Done on a Classwide Basis

Plaintiffs' and the class members' monetary relief is "capable of measurement on a classwide basis." *Comcast Corp. v. Behrend*, 133 S. Ct. 1426, 1433 (2013). "The amount of damages is invariably an individual question and does not defeat class action treatment." *Blackie v. Barrack*, 524 F.2d 891, 905 (9th Cir. 1975); *see also Leyva v. Medline Indus. Inc*., 716 F.3d 510, 513-14 (9th Cir. 2013) (holding that the district court abused its discretion in finding that individualized issues of damages precluded class certification).

Both ECPA and CIPA provide for statutory damages. 18 U.S.C. § 2520(c)(2); Cal. Pen. Code § 637.2. Federal courts "regularly recognize the superiority of class litigation in suits for statutory damages." *Holloway v. Full Spectrum Lending*, 976 F.2d 497, *8-9 (C.D. Cal. 2007). Moreover, the Ninth Circuit clearly states that the superiority analysis does not change when the size of the class creates an excessively large damages model. *Bateman v. Am. Multi-Cinema, Inc*., 623 F.3d 708, 721 (9th Cir. 2010) ("enormous" aggregate damages liability "is not an appropriate reason to deny class certification under Rule 23(b)(3)."). Instead, "the district court may be entitled to reduce the award if it is unconstitutionally excessive…but constitutional limits are best applied after a class has been certified." *Id*. at 723 (quoting *Murray v. GMAC Mortg. Corp*., 434 F.3d 948, 954 (7th Cir. Ill. 2006)). The Seventh Circuit further clarifies the policy

[54] Facebook Form 10-K for the fiscal year ended December 31, 2013. (available at http://www.sec.gov/Archives/edgar/data/1326801/000132680114000007/fb-12312013x10k.htm).
[55] Ex. 31 (Pltfs.' First Set Requests for Prod.), Request No. 29 (seeking "[a]ll Documents and ESI related to – and sufficient to identify – the 'dedicated team of privacy professionals' identified on page 8 of Your Form 10-K for fiscal year ending December 31, 2013.")
[56] Ex. 32 (Ltr. from Joshua Jessen to Hank Bates, April 10, 2015), at 1 ("With respect to Request No. 29, please be advised that there is no specific list of the 'dedicated team of privacy professionals' referenced in the Request.").

underlying this holding: "[C]onstitutional limits are best applied after a class has been certified. Then a judge may evaluate the defendant's overall conduct and control its total exposure. Reducing recoveries by forcing everyone to litigate independently—so that constitutional bounds are not tested, because the statute cannot be enforced by more than a handful of victims—has little to recommend it." *Murray*, 434 F.3d at 954.

ECPA also authorizes "equitable…relief as may be appropriate," as well as "profits made by the violator as a result of the violation." 18 U.S.C. § 2520(b)(1), (c)(2). Plaintiffs can offer common proof to calculate the value which Facebook derived from intercepting private message content, as well as a method for an equitable allocation of those ill-gotten gains to the members of the class. *See* Ex. 33, Report of Fernando Torres in Support of Plaintiffs' Motion for Class Certification ("Torres Report"). Through interceptions of private messages, Facebook creates related Objects and Associations which populate Facebook's Social Graph. *Id*. at ¶ 23. Facebook's Social Graph represents the integration of information collected by Facebook about Facebook users, and encompasses their location, demographics, interests, behaviors, and connections. *Id*. at ¶ 21. The unlawfully intercepted private message content contributes meaningful data to the Social Graph, increasing the quality of its ability to provide predictive value, and, consequently, increasing Facebook's advertising revenue and value. *Id*. at ¶¶ 36 *et seq*. A reasonable value to Facebook of the intercepted content can be assigned on a per URL basis, and can be allocated to class members on that basis. *Id*. at ¶ 60.

In addition, Facebook generated value from its inflation of third-party Like counters. The economic benefit derived by Facebook attributable to this conduct 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. *Id*. at ¶ 63. Again, the value of these Likes can be allocated to class members based upon Facebook's data which retains user-specific logs for each artificially derived Like. *Id*. at ¶ 73.

2. A Class Action Is Superior to Any Alternative

The "objectives of the particular class action procedure will be achieved in th[is] particular case," making class certification the superior method for litigating class members'

claims. *Hanlon*, 150 F.3d at 1023. Here, a class action is the only mechanism by which Plaintiffs and class members can practically vindicate the privacy interest at issue, as it stands in direct conflict with the business model of one of the world's largest corporations.[57] The resources required to litigate these claims could never sustain an individual action against Facebook.[58] Accordingly, absent class certification, the boundaries of permissible private surveillance, established by the Common Law and embodied in ECPA and CIPA, will go unenforced and will likely be breached with impunity. As electronic communications through social media such as Facebook become the dominant mode of interpersonal communication, the need for proper boundaries has never been more important. *See, e.g.*, J. Cohen, *What Privacy Is For*, 126 Harv. L. Rev. 1904, 1927-32 (2013).

3. <u>This Class Action Is Manageable</u>

Class-wide resolution of class members' claims will be manageable. First, all of the claims are governed by the same statutory laws. Second, the central issue of liability will hinge on the several categories of common proof outlined herein: Either Facebook intercepted messages in transit, or it did not; either Facebook's scanning devices were "being used in the ordinary course of its business," or they were not; either Facebook's public disclosures of its practice could have provided "actual knowledge," of the alleged violations, or they did not. Third, the potential measures of class-wide relief require common proof: statutory damages, profits resulting from Facebook's conduct, and/or other appropriate equitable relief. *See Six (6) Mexican Workers v. Az.*

---

[57] This weighing of fundamental privacy interests against corporate profit is exemplified by [redacted]'s comments in his investigation of the percentage of private message scans that contributed to Likes on third-party websites: "given the low contribution and high degree of scrutiny from privacy advocates, let's just remove it." Ex. 30 (FB000000502). Implicit in this analysis is the proposition that, had the counts been higher, economic interest would have warranted a continuation of the scans. Earlier, when Facebook believed that the contribution rate was larger, concern was expressed about abandoning the practice. *See, e.g.*, Ex. 34 (FB00000802) ("[A]re we seeing from these samples are seeing [sic] btwn 18-29% likes through private messages? That seems huge? Think it makes sense to ask [redacted] about it. I mentioned this to [redacted] and he was surprised that it acted in this way. Will these news sites see their Likes go down by 20% if we stop this going forward?")

[58] *See* Declaration of Joshua Jessen in Support of Defendant Facebook, Inc.'s Opposition to Plaintiffs' Renewed Motion to Continue Deadlines (Dkt. 135-1) (detailing, generally, productions occurring from February, 2015 through the end of October, 2015; discovery disputes resolved by Magistrate Judge Maria-Elena James; and the fact that "Plaintiffs and their experts have collectively spent 48 days reviewing Facebook's source code.").

Citrus Growers, 904 F.2d 1301, 1306 (9th Cir. 1990) (affirming class certification, explaining that individualized proof manageability issues "are not at issue where the underlying statute permits awards without a showing of actual damage."). "Indeed, the only difficulties likely to be encountered in this case would result from not certifying the class, given the expenditure of time and resources that would result—from both the court's and the parties' perspectives—in requiring each class member's action to proceed independently." *In re Online DVD Rental Antitrust Litig.*, No. 09-2029, 2010 WL 5396064, at *12 (N.D. Cal. Dec. 23, 2010) (Hamilton, J.) *aff'd*, 779 F.3d 934 (9th Cir. 2015).[59]

C. Alternatively, Class Certification Under Rule 23(b)(2) Is Appropriate

A class may be certified pursuant to Fed. R. Civ. P. 23(b)(2) when plaintiffs "complain of a pattern or practice that is generally applicable to the class as a whole.'" *Rodriguez*, 591 F.3d, at 1125 (quoting *Walters v. Reno*, 145 F.3d 1032, 1047 (9th Cir. 1998)); Fed. R. Civ. P. 23(b)(2). The conduct Plaintiffs challenge in this litigation—Facebook's scanning, intercepting, cataloging, and using of private message content—affects all class members uniformly and has been implemented in a way that violated class members' legal rights identically and consistently. *Yahoo Mail Litig*. (certifying a class under Rule 23(b)(2) where "[p]laintiffs contend that all emails sent from and to Yahoo Mail subscribers are subject to the same interception and scanning processes [and thus] challenge a pattern or practice that is generally applicable to the class as a whole.") 308 F.R.D. at 598 (internal citations, quotations omitted). Further, the relief sought—cessation of the practice, destruction of any records created from illegally-obtained private message content, and a declaration that such conduct violates ECPA and CIPA—would benefit the class as a whole. *Id*. ("Moreover, Plaintiffs seek only injunctive and declaratory relief, which is appropriate under Rule 23(b)(2).") (citations omitted). Accordingly, as an alternative to certification pursuant to Rule 23(b)(3), the Court should allow the class to seek injunctive and declaratory relief pursuant to Rule 23(b)(2).

[59] The superiority and manageability of the proposed class proceeding are so straightforward that a trial plan is self-evident. *See Karim v. Hewlett-Packard Co.*, No. 12-5240, 2014 WL 555934, at *7 (N.D. Cal. Feb. 10, 2014) (Hamilton, J.) (certifying class action because superiority is self-evident even without a trial plan).

V. CONCLUSION

Plaintiffs request that the Court grant their motion for class certification, appoint Matthew Campbell and Michael Hurley as class representatives, and appoint Lieff Cabraser Heimann & Bernstein and Carney Bates & Pulliam as class counsel.

Dated: November 13, 2015

Lieff Cabraser Heimann & Bernstein, LLP

By: /s/ *Michael W. Sobol*
Michael W. Sobol

Michael W. Sobol (State Bar No. 194857)
msobol@lchb.com
David T. Rudolph (State Bar No. 233457)
drudolph@lchb.com
Melissa Gardner (State Bar No. 289096)
mgardner@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

Rachel Geman
rgeman@lchb.com
Nicholas Diamand
ndiamand@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
250 Hudson Street, 8th Floor
New York, NY 10013-1413
Telephone: 212.355.9500
Facsimile: 212.355.9592

Hank Bates (State Bar No. 167688)
hbates@cbplaw.com
Allen Carney
acarney@cbplaw.com
David Slade
dslade@cbplaw.com
CARNEY BATES & PULLIAM, PLLC
11311 Arcade Drive
Little Rock, AR 72212
Telephone: 501.312.8500
Facsimile: 501.312.8505

Attorneys for Plaintiffs and the Proposed Class