David M. Given (SBN 142375)
Nicholas A. Carlin (SBN 112532)
**PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP**
39 Mesa Street, Suite 201
The Presidio
San Francisco, CA 94129
Tel: 415-398-0900
Fax: 415-398-0911
Email: dmg@phillaw.com
Email: nac@phillaw.com

*Interim Co-Lead Counsel for Plaintiffs*
[ADDITIONAL COUNSEL LISTED BELOW]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MARK OPPERMAN, et al.,

Plaintiffs,

v.

PATH, INC., et al.,

Defendants.

Case No. 13-cv-00453-JST

**UNREDACTED VERSION OF PLAINTIFFS' NOTICE OF MOTION AND MOTION FOR CLASS CERTIFICATION RE FOURSQUARE, INSTAGRAM, KIK, TWITTER AND YELP APPS; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF**

Date: Nov. 15, 2016
Time: 9:30 a.m.
Ctrm: 9, 19th Floor

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

## TABLE OF CONTENTS

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

## TABLE OF AUTHORITIES

**PAGE(S)**

### Cases



### Other Authorities

**Rules**



PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

**TO THE COURT, ALL PARTIES, AND COUNSEL OF RECORD:**

**PLEASE TAKE NOTICE** that on Nov. 15, 2016, at 9:30 AM, or as soon thereafter as the matter may be heard, in Courtroom 9, 19th Floor of the United States District Courthouse, 450 Golden Gate Avenue, San Francisco, California, 94102, before the Honorable Jon S. Tigar, Plaintiffs Giuliana Biondi, Stephanie Cooley, Jason Green, Claire Hodgins, Gentry Hoffman, Rachelle King, Nirali Mandalaywala, and Judy Paul (hereinafter, "Plaintiffs"), on their own and on behalf of the putative classes (as defined below), will and hereby do move this Court for an Order: (1) granting class certification in the above-captioned action ("Action") against Defendants FOURSQUARE LABS, INC., INSTAGRAM, LLC, KIK INTERACTIVE, INC., TWITTER, INC. and YELP INC. (collectively, the "App Defendants") as well as against APPLE, INC. (together with the App Defendants, collectively, "Defendants"), pursuant to Rule 23(a) and (b)(3) of the Federal Rules of Civil Procedure; (2) appointing Plaintiffs as Class Representatives; and (3) appointing Plaintiffs' Interim Co-Lead Counsel (hereinafter, "Plaintiffs' Counsel") as Class Counsel.

This Motion is based upon this Notice of Motion and Motion, the attached Memorandum of Points and Authorities, the accompanying Declaration of Diana C. Buck and exhibits thereto, the accompanying Declaration of Arno Puder, Ph.D., the accompanying declarations of Plaintiffs and the exhibits thereto, the Declarations of David M. Given and Michael von Loewenfeldt (submitted with the accompanying class certification motion against Apple on the "Tobacco II" claims), the papers and records on file in this Action, and such other written and oral arguments as may be presented at or before the hearing to the Court.

## MEMORANDUM OF POINTS AND AUTHORITIES

## I. INTRODUCTION

Plaintiffs (as identified in the parentheticals below) move to certify the following classes against the App Defendants on Plaintiffs' claim for invasion of privacy/intrusion on seclusion and against Apple for aiding and abetting the same:

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

**The Foursquare App Class** (by Plaintiffs Paul, Mandalaywala and King): All persons in the U.S. who received from Apple's App Store one or more of versions 1.1 through 4.2 of the iOS mobile application entitled Foursquare (the "Find Friends Versions"), and did one or more of the following between April 4, 2009 and February 8, 2012 (the "Foursquare Class Period"): (1) for versions 1.1 through 4.2, activated via their Apple iDevice (iPhone, iPad, iPod Touch) the "Add Friends" feature; or (2) for versions 3.1 through 4.2, registered via their iDevice as a Foursquare user through those Find Friend Versions.

**The Instagram App Class** (by Plaintiffs Biondi and Mandalaywala): All persons in the U.S. who received from Apple's App Store a copy of versions 1.0.0 through 2.0.7 of the iOS mobile application entitled Instagram (the "Find Friends Versions") and activated via their Apple iDevice (iPhone, iPad, iPod Touch) the "Find Friends" feature of a Find Friends Version between Oct. 6, 2010 and Feb. 8, 2012 (the "Instagram Class Period").

**The Kik App Class** (by Plaintiffs Cooley and Green): All persons in the U.S. who received from Apple's App Store one or more of versions 2.2.0 through 5.5.4 of the iOS mobile application entitled Kik Messenger (the "Find Friends Versions"), and did one or more of the following between October 19, 2010 and February 8, 2012 (the "Kik Class Period"): (1) for versions 2.2.0 and 2.2.1, launched via their Apple iDevice (iPhone, iPad, iPod Touch) one of those two Find Friends Versions; or (2) for the versions 2.2.2 through 5.5.4, activated via their Apple iDevice the "Find Friends" feature.

**The Twitter App Class** (by Plaintiffs Biondi, Hodgins, King, and Mandalaywala): All persons in the U.S. who received preinstalled on an Apple iDevice and/or from Apple's App Store a copy of versions 3.3 through 4.0.1 of the iOS mobile application entitled Twitter (the "Find Friends Versions") and activated via their Apple iDevice (iPhone, iPad, iPod Touch) the "Find Friends" feature of a Find Friends Version between March 3, 2011 and Feb. 8, 2012 (the "Twitter Class Period").

**The Yelp App Class** (by Plaintiffs Hodgins, Hoffman and Mandalaywala): All persons in the U.S. who received from Apple's App Store a copy of versions 4.0.0 through 5.6.0 of the iOS mobile application entitled Yelp (the "Find Friends Versions") and activated via their Apple iDevice (iPhone, iPad, iPod Touch) the "Find Friends" feature of a Find Friends Version between Jan. 16, 2010 and Feb. 8, 2012 (the "Yelp Class Period").

The above definitions identify an objective, ascertainable and numerous group of people as to each of the proposed classes. Plaintiffs' privacy claim arises from Defendants' uniform (and therefore common) course of conduct directed at those people. See ECF No. 761 ("Path App Order"), at 6-7.

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

Those people's Contacts data is private. See Path App Order, at 18. More to the point, as Apple concedes, that data is private property. See ECF No. 1-2, at 25 (the "Address Book database is ultimately owned by the user").

The definition of private property is the right to exclude. *Rakas v. Illinois*, 439 U.S. 128, 143 & n.12 (1978). Notwithstanding Apple's unqualified acknowledgement of its customers' rights, however, Apple left the door to that property wide open. See ECF No. 651-1 [Kennedy Decl.], at ¶ 21 & Ex. Q (developers "can obtain [Contacts data] without user interaction"). And when the time came, Apple walked the App Defendants right through that door. See, e.g., Section II.D., below.

Defendants' course of conduct resulted in one or more privacy violations uniform across the proposed classes, resulting in a uniform measure of damage. The factual and legal issues giving rise to Plaintiffs' claims predominate. See Path App Order, at 28.

Because their respective claims against Defendants are typical of those of the class, Plaintiffs can and will adequately protect the interests of the proposed classes in a representative capacity. Plaintiffs therefore move to certify the above classes pursuant to Rule 23(a) and 23(b)(3), appoint Plaintiffs as Class Representatives, and appoint Plaintiffs' Counsel as Class Counsel pursuant to Rule 23(g)(1).

## II. STATEMENT OF ISSUE TO BE DECIDED

Applying the Federal Rules of Civil Procedure, whether the Court will certify one or more of the classes in this Action as proposed above.

## III. STATEMENT OF CLASS-WIDE FACTS

The mobile device applications at issue for each of the App Defendants obtained private address book (or "Contacts") data and sent that data to each of the respective App Defendants' servers without consent from every user in the proposed classes. (The Court's background on Contacts explains the salient features of the Apple-developed address book database pre-installed with every iDevice in issue. See Path App Order, at 1-2; see also ECF No. 651-1 [Kennedy Decl.], at ¶ 28 & Exh. X). With Apple's knowledge and assistance, the App Defendants created and distributed their apps (the popular shorthand for "mobile device

applications") that without adequate notice or express permission harvested the Contacts database of class members.

The fact issues likely to resolve Plaintiffs' and the putative class members' invasion of privacy claims against each of the App Defendants are common to each proposed class. Moreover, on a class-by-class basis specific to each App Defendant and Apple, those issues are subject to proof by the same documents and percipient and expert testimony.

By obtaining private data without consent, the App Defendants more rapidly grew their social graphs and enhanced their social networking features, increasing the value of their user data and therefore their respective companies. Apple explained this value proposition when it filed a patent for a social graph application: "Matching algorithms can then use the profile or data provided to match members with members who are deemed compatible by the algorithms, under the assumption, for example, that matching people's interests and values can lead to successful new friendships or relationships ***within the social network***." See U.S. Patent No. 8,386,620 col.1 (filed Dec. 15, 2009) (emphasis added); Buck Decl. at ¶ 2 & Exh. A.

Consistent with Apple's description, the App Defendants' treatment of their Find Friends data after the class period shows that they gained a competitive edge by building up their social graphs in secret. In July 2012, Twitter cut off Instagram from its "find friends" graph, saying: "We understand that there's great value associated with Twitter's follow graph data, and we can confirm that it is no longer available within Instagram." Buck Decl. at ¶ 3 & Exh. C.

One month later, Twitter extended a similar ban against social media platform Tumblr and pointed the media to its prior "great value" press statement. Buck Decl. at ¶ 4 & Exh. C. For its part, Instagram cut off a startup TIINY from its "find friends" social graph. Buck Decl. at ¶ 5 & Exh. D. By hiding the data flow from the user to the App Defendants' servers, the App Defendants avoided the costs of social graph acquisition (i.e. a user's resistance to giving up control over her address book data), in violation of law.

Two of the App Defendants, Kik and Foursquare, created and distributed versions of their apps designed to harvest from class members' iDevices massive amounts of private address book data and sent that data to their web servers without any user prompt or privacy policy

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

disclosure whatsoever. See Path App Order, at 2. The Kik app obtained all Kik users' Contacts' emails and phone numbers between Oct. 19, 2010 and Dec. 6, 2010 upon registration. Buck Decl. at ¶ 11 & Exh. J at 7-8, 13-14 (Kik Supp Rogs 1, 5); see ECF No. 500-1 [Heinke Decl.], at ¶¶ 3, 6-7 & Exhs. C & D. Foursquare obtained each newly registered user's Contacts' first name, last name, email address, and phone numbers, between May 24, 2011 and Feb. 14, 2012. Buck Decl. at ¶ 8 & Exh. G at 8-10 (Foursquare Rog 3).

The other App Defendants (and Kik and Foursquare during other periods of time) also took tens of billions of records from users' Contacts data without obtaining proper consent to do so. Each of the App Defendants have suggested in prior pleadings that Plaintiffs and putative class members consented to an upload of their data by agreeing to a "scan" of their Contacts, or to "Add" or "Find" their friends from their iDevice's Contacts data base. Buck Decl. at ¶¶ 7–10 & Exhs. F-I (Instagram Supp Rog 3, Foursquare Rog 3, Twitter Supp Rog 3, Yelp Supp Rog 3); see ECF No. 500-1 [Heinke Decl.], ¶ 7 at Exh. D. The App Defendants argue that, by tapping on a "scan" notification, users consented to their data being taken off their iDevices – a common question that will have the same answer for all members of each of the proposed classes.

Mobile iOS apps should not transmit data off a user's device without express permission. Section 17.1 of Apple's 2010 data privacy rules say: "Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used." See ECF No. 651-1 [Kennedy Decl.], at ¶ 19 & Exh. O.

Despite this common sense user expectation, as reinforced by Apple's public guarantees, the App Defendants used deliberately misleading words like "scan" but then did not just access Contacts data, they copied that data and sent themselves a copy over the internet. Puder Decl. at ¶¶ 15-17; Buck Decl. at ¶¶ 7-11 & Exhs. F-J (Instagram Supp Rog 3, Foursquare Rog 3, Twitter Supp Rog 3, Yelp Supp Rog 3, Kik Supp Rog 3). As one Twitter employee stated internally during the Twitter Class Period, acknowledging the qualitative difference: "'find friends' was always confusing (it really means 'import contacts')." Buck Decl. at ¶ 23 & Exh. V (Bates No. TWITTER_07342).

Each of the App Defendants coded their apps to secretly activate a function built into Apple's operating software allowing the wholesale transmission of Contacts data. Puder Decl. at ¶¶ 4, 16; Buck Decl. at ¶¶ 7–11 & Exhs. F-J (Instagram Supp Rog 3, Foursquare Rog 3, Twitter Supp Rog 3, Yelp Supp Rog 3, Kik Supp Rog 3). These weren't leaks – the App Defendants coded the data harvesting functions into their apps, as permitted (and encouraged) by Apple, but designed user prompts to disguise what was actually happening. See ECF No. 502-8 [iOS User Interface Guidelines], at ¶ 56 (encouraging developers to "[g]et information from iOS, when appropriate. People store lots of information on their devices. When it makes sense, don't force people to give you information you can easily find for yourself, such as their contacts or calendar information.").

[redacted] Buck Decl. at ¶ 22 & Exh. U (Bates No. TWITTER_06489). [redacted] Buck Decl. at ¶ 24 & Exh. W (Bates No. TWITTER_07568).

The App Defendants made a deliberate choice not to seek user permission to upload data. The motive for this could not be clearer: [redacted] Buck Decl. at ¶ 24 & Exh. W (Bates No. TWITTER_07568).

Kik's CEO expressed the same intent: to hide the code-level design of his company's app from Kik's users, even after Apple rejected Kik's app for violating Rule 17.1. Buck Decl. at ¶ 20 & Exh. S (Bates No. Kik_117). "Are we *required* to show a dialog?" he asked his direct reports in May of 2011, "Apple made us do it because of the 'controversy', but they let it slide without *anything* once." Buck Decl. at ¶ 20 & Exh. S (Bates No. Kik_117).

The upload function used by these apps was not merely invasive – in many cases it violated computer security best practices. Puder Decl. at ¶¶ 7-9. While some of the App Defendants transmitted address book data over a secure, encrypted connection, most did not.

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

See ECF No. 727-1, [Puder (Re Yelp) Decl.], at ¶ 9; Buck Decl. at ¶¶ 7-9, 11 & Exhs. F-H, J (Instagram Supp Rog 3, Foursquare Rog 3, Twitter Supp Rog 3, Kik Supp Rog 3).

None of the App Defendants used a popular and industry-standard security technique called "hashing" to protect their users' data during transfer. Puder Decl. at ¶¶ 6 & 18; Buck Decl. at ¶ 7-9 & 11 & Exh. F-H & J (Instagram Supp Rog 3, Foursquare Rog 3, Twitter Supp Rog 3, Kik Supp Rog 3). See also ECF No. 727-1, [Puder (Re Yelp) Decl.], at ¶ 5 et seq. Lack of hashing is strongly indicative of the App Defendants' motive and objective in this, i.e., acquisition of useable, intact data. Regardless of their security measures, the relevant computer code shows conclusively, in a manner common to all users, that each of the App Defendants sent their customers' data back to their own servers throughout the class period without adequate notice or anything approaching informed consent to upload.

**A. Foursquare**

Foursquare published a location app (also called Foursquare) that obtained address book data from class members through two separate channels within the app: the registration flow for new users and the "profile" tab for users who were already registered. Buck Decl. at ¶ 8 & Exh. G at 8-10 (Foursquare Rog 3).

As noted, Foursquare uploaded all of the email addresses and phone numbers from new registrants' Contacts between May 24, 2011 and Feb. 8, 2012, in the background with no prompt at all. Puder Decl. at ¶¶ 3-6; Buck Decl. at ¶ 8 & Exh. G at 8-10 (Foursquare Rog 3). Between those dates, Foursquare forced every new registrant into a "Find Friends" screen immediately after registering. Puder Decl. at ¶¶ 3-6. [redacted]

For registered users, Foursquare obtained address book data after presenting a "scan" prompt. Buck Decl. at ¶ 8 & Exh. G at 4-10 (Foursquare Rogs Nos. 1-3). The "profile tab" told users to "Scan my address book" between April 2009 and Feb. 8, 2012. Buck Decl. at ¶ 8 & Exh. G at 4-10 (Foursquare Rogs Nos. 1-3). Instead of a scan, Foursquare would upload all

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

contacts' email addresses and phone numbers directly to Foursquare's servers. Buck Decl. at ¶ 8 & Exh. G at 10-11 (Foursquare Rog 5).

While Foursquare was configured to transmit this contact information over an encrypted line, the data was transmitted without hashing. Puder Dec. at ¶¶ 6, 7; Buck Decl. at ¶ 8 & Exh. G at 11 (Foursquare Rog 6). Foursquare only began encrypting the connection over which the data was sent in Aug. 2010. Buck Decl. at ¶ 8 & Exh. G at 11 (Foursquare Rog 6).

[redacted]

**B. Instagram**

Instagram published an image sharing app (also called Instagram) that prompted users to "Find Friends," between Oct. 6, 2010 and Feb. 8, 2012. Instagram users encountered prompts that offered to "Find Friends from my Contact List." Puder Decl. at ¶¶ 13, 21; Buck Decl. at ¶ 7, 18 & Exhs. F at 10-12, Q (Instagram Supp Rog 3; INSTAGRAM_609). Instagram used this prompt to send each user's contacts data—first names, last names, email addresses, and phone numbers—directly to Instagram.[1] Buck Decl. at ¶ 7, 17 & Exhs. F at 10-12, P (Instagram SUPP. Rog 3; INSTAGRAM_173.)

As evidence that this disclosure was inadequate (and of Instagram's culpable state of mind), Instagram misrepresented the extent of its disclosures to users in an April 2012 letter to Congress, once Instagram's surreptitious upload of this data was publicized. In a letter to Representatives Henry A. Waxman and G.K. Butterfield, Instagram CEO Kevin Systrom stated that all users during the Instagram Class Period (as defined above) received a "real-time, pop-up notice screen and explicit warning" that states "In order to find your friends, we need to send address book information to Instagram's servers using a secure connection." Buck Decl. at ¶ 18 & Exh. Q at 3 (INSTAGRAM_609). In fact, source code review reveals, this prompt was not present in any version of Instagram prior to Feb. 2012. Puder Decl. at ¶ 14.

[1] Plaintiffs include here a visual example of the data, sent directly to Instagram's CEO at the beginning of the Instagram Class Period. Buck Decl. at ¶ 17 & Exh. P (INSTAGRAM_163-270.) The interest of Instagram's highest-level executive in the acquisition of this data is informative of the value Instagram put on this function.

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

The data was sent back to Instagram servers in an unhashed, readable form. *See, e.g.*, Buck Decl. at ¶¶ 17, 18 & Exhs. P, Q (INSTAGRAM_163-270; 609-10). Instagram does not claim to have encrypted the data before sending it back to its servers. Buck Decl. at ¶ 7 & Exh. F at 15-16 (Instagram SUPP Rog 6).

Instagram intended to mine the data for social graphing insights. Buck Decl. at ¶ 18 & Exh. Q at 4 (INSTAGRAM_610) ("for the purpose of a more useful service"). Once on Instagram's servers, Instagram stored the data to determine its usefulness. Buck Decl. at ¶ 18 & Exh. Q at 4 (INSTAGRAM_610). While Instagram stated to Congress that it terminated its storage function on July 28, 2011, Instagram's code production showed that Instagram maintained the ability to execute the same storage function in its server code through the end of the Instagram Class Period in Feb. 2012. Puder Decl. at ¶¶ 19-25.

Instagram approximates that 8,463,326 individuals registered for the Instagram App during the class period within the U.S. Buck Decl. at ¶ 7 & Exh. F at 23-27 (Instagram Supp Rog 12.)

**C. Kik**

Kik published a messaging app (called Kik Messenger) that prompted users to "use your address book" to Find Friends. At all relevant times, Apple knew that Kik was uploading email addresses and phone numbers and never required Kik to explain the extent to which Kik was obtaining address book data. Buck Decl. at ¶ 13 & Exh. L (Bates No. APL-PATH_32230).

Between Oct. 19, 2010 and Dec. 6, 2010, Versions 2.2.0 and 2.2.1 of the Kik app uploaded email addresses and phone numbers from the user's address book to Kik's servers upon registration (a la the Path App). Buck Decl. at ¶ 11 & Exh. J at 7-8, 13-14 (Kik Supp Rogs Nos 1 and 5). Apple reviewed Kik Messenger on Nov. 9, 2010. Buck Decl. at ¶ 13 & Exh. L (Bates No. APL-PATH_32230).

Apple created an address book with "fake contacts" ("some with names and numbers") and tested the Kik App's collection of address book data. Buck Decl. at ¶ 13 & Exh. L (Bates No. APL-PATH_32230). Once Apple determined Kik was not asking for permission prior to collecting the data, Apple concluded that Kik was violating Rule 17.1 of its publicly available

consent rules and rejected the application. Buck Decl. at ¶ 13 & Exh. CC (Bates No. APL-PATH_32230).

Starting with Version 2.2.2, publicly available on Dec. 6, 2010, and through to Feb. 8, 2012, the Kik app prompted users to "use your address book to tell you which of your friends" are already using the Kik service. Buck Decl. at ¶ 12 & Exh. K (Bates No. APL-PATH_17762); ECF No. 500-1 [Heinke Decl.], ¶ 7 & Exh. D ("'Kik Messenger' would like to access your address book to match you with friends already on Kik"). Once this function ran, Kik transmitted email addresses and phone numbers from the user's address book to Kik's servers. Buck Decl. at ¶ 11 & Exh. J at 13-14 (Kik Supp Rog 5). The data was sent back to Kik servers in an unhashed, readable form. Buck Decl. at ¶ 11 & Exh. J at 13-14 (Kik Supp Rog 5).

**D. Twitter**

Twitter published a blogging app that was "native" to iOS (pre-installed by Apple in all new iDevices) that between March 3, 2011 and Feb. 8, 2012, incorporated a "Find Friends" prompt. Buck Decl. at ¶ 9 & Exh. H at 3-5 (Twitter Supp Rogs 1 and 2). The Twitter app prompted new Twitter users with a sign-up display that offered to: "Scan your contacts." Buck Decl. at ¶ 9 & Exh. H at 5-8 (Twitter Supp Rog 3.) Once the user opted to scan his or her contacts, the email and phone number of each contact would be sent, separately, to a Twitter server. Buck Decl. at ¶ 9 & Exh. H at 5-8 (Twitter Supp Rog 3).

The information would be stored for 18 months, or until users deleted their accounts. Buck Decl. at ¶ 9, Exh. H at 9, 13-14, 20-12 (Twitter Rogs 5, 9, 18). Twitter first developed a feature that allowed for users to delete their address books from Twitter's servers in Jan. 2012. At that point, one Twitter product manager stated: "[I] have a feeling the legal team just had a sigh of relief :)" Buck Decl. at ¶ 28 & Exh AA (TWITTER_10225).

[redacted] *See, e.g.*, Buck Decl. at ¶ 21 & Exh. T (Bates No. TWITTER_05756.) [redacted] *Id.*

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

[redacted] Buck Decl. at ¶ 24 & Exh. W (Bates No. TWITTER_07568). Guido van Rossum published a Google+ blog post that described Twitter's use of address book data, stating: "But lo and behold, as soon as I clicked, the Twitter app started sending my entire address book to the Twitter servers and displaying matches -- *without* first asking me if that's what I wanted to do (I would have said no)." Buck Decl. at ¶ 6 & Exh. E.

Twitter's mobile product manager Sung Hu Kim commented on the blog post on his company's behalf and pointed to the "scan your contacts" prompt. Buck Decl. at ¶ 6 & Exh. E at 6. "Its intention was to make clear that we'd be reading the phone's address book as part of this feature," Kim stated in his comment. Buck Decl. at ¶ 6 & Exh. E at 6. [redacted] Buck Decl. at ¶ 24 & Exh. W (Bates No. TWITTER_07568).

The Twitter app and Twitter's Find Friends function within the app were the result of substantial cooperation between Twitter and Apple. Buck Decl. at ¶ 26, 27 & Exhs. Y, Z (Bates Nos. TWITTER_12639; TWITTER_22951). To supplement the Find Friends function in Twitter, Apple directly incorporated an accompanying function in the Contacts software itself, whereby Apple sent the same address book data to Twitter's servers using the following disclaimer language: "Twitter will use email addresses and phone numbers from your contacts to add Twitter user names and photos to your contact cards."

Apple managed that screen. *See* Buck Decl. at ¶ 26, 27 & Exhs. Y, Z (Bates Nos. TWITTER_12639; TWITTER_22951). Despite Apple's direct involvement in planning Twitter's address book upload, Apple did not mention its consent rules until at earliest Dec. 14, 2011, when Apple called Twitter and expressed its concern about "not giving users notice about what's happening." Buck Decl. at ¶ 25 & Exh. X (Bates No. Twitter_11523). It does not appear that message of concern changed any ongoing practice.

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

Twitter estimates that during the class period, [redacted] accounts utilized the "Find Friends" feature using one of its "find friends" versions. Buck Decl. at ¶ 9 & Exh. H at 16-17 (Twitter Supp Rog 12).

**E. Yelp**

Yelp implemented its Friend Finder function in version 4.0.0 of its mobile app (also called Yelp), released on Jan. 16, 2010, and it remained in effect through end of the class period on Feb. 8, 2012. Buck Decl. at ¶ 10 & Exh. I at 2-4 (Yelp Supp Rog 1). During the class period, Yelp prompted members of the class to "Find friends on Yelp using your Contacts and Facebook Friends?" Buck Decl. at ¶ 10 & Exh. I at 4-7 (Yelp Supp Rog 3).

If users selected "Yes, Find Friends," Yelp then transmitted email addresses contained in users' address books back to Yelp's servers. Buck Decl. at ¶ 10 & Exh. I at 4-7 (Yelp Supp Rog 3). Yelp did not hash the address book data before sending it back to its servers. See ECF 727-1 [Puder (Re Yelp) Decl.], at ¶ 5 et seq. Furthermore, while Yelp contends that the data was sent using an encrypted connection, a review of the code does not support that claim. *Id.*, at ¶ 9.

Yelp estimates that 831,151 unique users used the Friend Finder function on iOS between its introduction in 2009 and Feb. 9, 2012. Buck Decl. at ¶ 10 & Exh. I at 10 (Yelp Supp Rog 12).

## IV. STATEMENT OF FACTS SPECIFIC TO PLAINTIFFS

Apple App Store purchase histories show Plaintiffs each downloaded a Find Friends Version of the respective apps in issue. See generally Biondi Decl.; Cooley Decl.; Green Decl.; Hodgins Decl.; Hoffman Decl.; King Decl.; Mandalaywala Decl.; Paul Decl. Each of the Plaintiffs downloaded a Find Friends Version of each of the respective apps to an iDevice, registered for the App (as evidenced by their use of the App) and, with the possible exception of the Kik app, activated the charged function ("Find Friends," "Add Friends," etc.), in each case resulting in the surreptitious and insecure upload of private address book data.

## V. PROCEDURAL BACKGROUND

On June 27, 2014, Plaintiffs filed their operative pleading. See ECF No. 478. On March 23, 2015, following extensive briefing, the Court issued its Order denying various motions to

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

dismiss and finding, among other things, that Plaintiffs adequately pled a claim for invasion of privacy/intrusion on seclusion against the App Defendants and for aiding and abetting on the part of Apple in connection therewith. See ECF No. 543.

On July 15, 2016, the Court issued its Path App Order, granting class certification with respect to a class of Path App users against both Path and Apple. Plaintiffs focus their discussion of certification of their underlying invasion of privacy/intrusion on seclusion claim (and the aiding and abetting of same) against Defendants consistent with that decision.

## VI. ARGUMENT

### A. Applicable Legal Standards.

The Court has set out the applicable legal standard for the present motion, which Plaintiffs adopt here. See Path App Order, at 5.

### B. The Requirements of Rule 23(a) Are Met

The proposed classes meet all of the requirements for class certification, satisfying numerosity, commonality, typicality, adequacy, and ascertainability. See Fed. R. Civ. P. 23(a).

#### 1. Numerosity is Satisfied.

Plaintiffs satisfy the numerosity requirement under Rule 23(a)(1) as to each proposed class. See Section VI.B.5., below.

#### 2. Commonality is Satisfied.

Plaintiffs satisfy the commonality requirement under Rule 23(a)(2) as to each proposed class. See Path App Order, at 7 & n. 2.

#### 3. Plaintiffs' Claims are Typical of the Proposed Class(es).

Plaintiffs satisfy the typicality requirement under Rule 23(a)(3) as to each proposed class. See Path App Order, at 7-8.

Class members' claims need not be identical, or even substantially so. Under Rule 23(a)'s "permissive standards," representative plaintiffs are typical if their claims are "reasonably co-extensive with those of absent class members; they need not be substantially identical." *Parsons v. Ryan*, 754 F.3d 657, 685 (9th Cir. 2014) (internal quotation omitted). See also Path App Order, at 7 (citing *Parsons* and setting out three-part test).

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

Some Find Friends Versions of some of the App Defendants' apps operated differently from one another during pertinent class periods. For example, as noted, both the Foursquare App and the Kik App had Find Friends Versions that automated the upload of address book data both with and without a prompt, notice, or opportunity to opt-out.

Nonetheless, each App Defendant committed an intrusion on seclusion against Plaintiffs and class members alike as to each of the proposed classes. See Keenley, *How Many Injuries Does It Take – Article III Standing in the Class Action Context*, 95 California L. Rev. 849, 879 (2007) (discussing continued viability of holding in *La Mar v. H&B Novelty*, 489 F.2d 461 (9th Cir. 1973) and positing "that increasing claim aggregation ought always be allowed [] so long as the representative plaintiff can show a substantial likelihood that litigation of her claim will be practically dispositive of the other claims she wishes to prosecute"). Apple aided and abetted in that privacy violation. Plaintiffs are aware of no individualized defenses available to any Defendant likely to become the focus of the litigation.

**4. Plaintiffs Are Adequate Class Representatives.**

Plaintiffs satisfy the adequacy requirement of Rule 23(a)(4) as to each proposed class. See Path App Order, at 8-9. Neither Plaintiffs nor their counsel have any conflicts of interest with other class members, and both Plaintiffs and their counsel have prosecuted and intend to continue to prosecute this Action vigorously on behalf of the proposed classes. See generally Given Decl.; von Loewenfeldt Decl. Plaintiffs are a subset of the named plaintiffs in the Action who, Plaintiffs' Counsel believe, will adequately represent the proposed classes; additional class representatives are available if the Court finds they are needed.

**5. Ascertainability is Satisfied.**

Plaintiffs have proposed a precise, objective, and presently ascertainable class definition satisfying Rule 23(a) as to each App Defendant. See Path App Order, at 27 & n. 13.

Ascertainability requires objective criteria to define the Class but does not require positive identification of class members. *Lilly v. Jamba Juice Co.*, 308 F.R.D. 231, 238 (N.D. Cal. 2014). The cornerstone of ascertainability is a class definition that gives notice to putative

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

members. *Id.* Lack of perfect identification of the members of each proposed class (assuming that is the case here) is not a bar to certification of any one of them.

As previously briefed, the Apple App Store is a particularly robust platform for class notice and claims administration in cases of this kind. See ECF No. 651, at 25. This is especially so when it comes to so-called "micropayments" (read: nominal damages) for the taking of personal data. See Jaron Lanier, *Who Owns the Future?* (Simon & Shuster 2014) (identifying firms like App Defendants that convince users to give away valuable personal information in exchange for "free" services, thereby accruing large amounts of data at virtually no cost, and proposing an economy of digital micro- or "nano-payments" in exchange for data and other uncompensated contributions to them).

Apple possesses records showing each user who received (i.e., downloaded) the Find Friends Versions of the charged applications. "Apple's servers regularly record each app download by a particular accountholder from the App Store at or near the time of the download in the form contained at Exhibit D. It is Apple's regular practice to maintain app download records of this kind for each Apple customer account used to download apps from the App Store." See ECF No. 395-2 [O'Neil Decl.], at 4 (¶ 21.d.) & Ex. D. Evidence of the download of a Find Friends Version of a given app by an iDevice owner is strongly indicative of registration and use by that owner – and in the case of social-networking (or "sharing") apps like Instagram, for example, of activation of the Find Friends function.

Much of what follows on the ascertainability subject derives, as it must, from answers to discovery Plaintiffs propounded on the App Defendants. Those answers were compelled by Magistrate Judge Spero's Feb. 3, 2016 Order (see ECF No. 635, at 2), the result of an all-day meet and confer conference held at the courthouse under Judge Spero's supervision. As reflected in the respective supplemental interrogatory responses of the App Defendants (the original responses were less than useless – and only Foursquare bothered to verify any of its responses, Buck Decl. at ¶ 32), that court-ordered discovery was patently incomplete and arguably in defiance of the Court's order directing the App Defendants to give answers

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

"specifying, version-by-version," exact categories of pertinent information or "a detailed explanation as to why a precise number [or approximation of users] cannot be given."

Nonetheless, the additional evidence adduced to date from the App Defendants should permit the Court to identify the people who comprise each proposed class, as follows:

- The Foursquare App Class – [redacted] Foursquare fails to explain why it has figures for that period alone, but simple math should suffice to extrapolate from that figure should Foursquare be unable to retrieve additional data for entirety of the Foursquare Class Period. That calculation can be cross-checked against Foursquare's (and Apple's) download records, if necessary. Moreover, between versions 3.1 (available beginning May 24, 2011) and version 4.2 (available through the end of the Foursquare Class Period), every new registrant or user of the Foursquare App had his address book data uploaded to Foursquare's servers. Puder Decl. at ¶ 5. These latter users should be easily identifiable, in the same manner Path users were.
- The Instagram App Class – Instagram attests that approximately 8,463,326 individuals registered for the Instagram app during the Instagram Class Period. Buck Decl. at ¶ 7 & Exh. F at 23-27 (Instagram Supp Rog 12). Given that the Instagram App features a social networking site focused primarily on the sharing of user-generated images, it is more likely than not that substantially all of those registrants used the pertinent "Find Friends" function; Instagram does not contend otherwise.[2]

[2] On Saturday, Aug. 20th, Instagram took its fourth swipe at supplementing its interrogatory responses. Buck Decl. at ¶ 31 & Ex. DD. These responses remain unverified, and Instagram offers no explanation for either the serial answers about its own code or the timing of this hideously late disclosure – almost one year to the day after Plaintiffs first propounded these discovery requests. That timing precludes before today a complete analysis by Plaintiffs' expert of Instagram's new factual contentions or the additional source code as well as, importantly, the related design documentation and developer comments, now offered for review.

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

- The Kik App Class – Kik attests that its Kik app was downloaded about "five million times" during the Kik Class Period. Buck Decl. at ¶ 11 & Exh. J at 23-26 (Kik Supp Rog 12). Kik has acknowledged that it has records "relating to the number of registered Kik accounts that utilized the Find Friends feature" for a four-month period during the Kik Class Period (although, like Foursquare, it fails to explain why it has figures for just that period), and those accounts total 999,642. Buck Decl. at ¶ 11 & Exh. J at 23-26 (Kik Supp Rog 12).
- The Twitter App Class – Twitter estimates that during the Twitter Class Period, [redacted] accounts utilized the "Find Friends" feature using one of the Find Friend Versions of the Twitter App. Buck Decl. at ¶ 9 & Exh. H at 16-17 (Twitter Supp Rog 12). Twitter can identify the specific or "unique" users who employed the "Find Friends" feature during the Twitter Class Period. See ECF No. 725-14 [Smith Decl.], at 8, et seq. (¶¶ 16-18).
- The Yelp App Class – Yelp estimates that 831,151 unique users used the "Friend Finder" function on iOS during the Yelp Class Period. Buck Decl. at ¶ 10 & Exh. I at 10 (Yelp Supp Rog 12).

While some of the App Defendants' discovery responses may fail to reflect the exact number or precise identity of members of a given app class as defined, notice to those who received from Apple a Find Friends Version (as defined for each of the App Defendants) provides an opportunity for cross-check with Apple's download records to correct any incomplete App Defendant records for people who claim membership in a class. For instance, such cross-check would allow sorting out those who downloaded a non-iOS version or downloaded to a non-iDevice.

In addition, evidence adduced in discovery confirms that one or more App Defendants uploaded and stored a user's "Unique Device Identifier." See, e.g., Buck Decl. at ¶ 30 & Exh BB (APL-PATH_18253). Apple knew about this practice throughout the proposed class periods. Buck Decl. at ¶ 29 & Exh. M (APL-PATH_00018321-22) ("For the record ALL apps are in violation as they send [UDID] data."). A UDID (its common acronym) – a sequence of

40 letters and numbers specific to a given iDevice – permits an App Defendant to determine that the user associated therewith used an iDevice. See *In re iPhone/iPad App. Consumer Privacy Litig.*, No. 11-MD-2250 LHK PSG, 2012 WL 5897351, at *6 (N.D. Cal. Nov. 21, 2012) ("according to Apple, the UDID is the means by which the data the devices collects can personally identify the device user").

While a few App Defendants claim they do not currently have readily-available records showing precisely which users triggered Find Friends, additional discovery may reveal methods to obtain the information (via commonly-employed database queries or, alternatively simple, automated programs to retrieve that data called "scripts") from Defendants' records. Notably, notwithstanding their interrogatory responses, no App Defendant has sworn it could not discover the precise identities of those users employing such queries or scripts.

Even if certain App Defendants did not keep records as to whose Contacts were taken, and whose existing records do not reveal the specific identity of those users, a class is still ascertainable under Rule 23. In each instance recited above, the outside number of members of each proposed class (i.e., the number of registered users of a given app's Find Friends Version) is known, and a subset thereof can be calculated with reasonable certainty.

From that figure, Plaintiffs can calculate damages on a per member (nominal) basis. At that point, a simple affidavit or claim form delivered via email can be used to confirm membership in the respective class. Cf. *Brown v. Hain Celestial Group*, 2014 WL 6483216, *11 (N.D. Cal. 2014) ("That self-identification is allowable here is bolstered by the fact that 'total damages' will be proved and fixed at trial – as opposed to awaiting a world of individual claimants who drive the defendant's bill higher with every new 'me too' that rings in.").

Many courts (including this one) have recognized that such confirmation proceedings are appropriate, particularly where (as here) the individual amounts at issue are small and the absence of records was caused by Defendant's choice not to keep records of its own misconduct. *Lilly*, 308 F.R.D. at 238-40 (responses to class notice that rely on applicant's "self-identification" do not preclude ascertainability finding). See also *Melgar v. CSK Auto*, 2015 WL 9303977, at *8-9 (N.D. Cal. Dec. 22, 2015) ("the need to rely on self-identification is a

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

problem of [defendant's] own making"); *Patel v. Trans Union*, 308 F.R.D. 292, 303 (N.D. Cal. 2015) ("The Northern District regularly certifies small-ticket consumer classes based on subjective self-identification in cases where the consumers' recall about purchases is accurate."); *Morales v. Kraft Foods*, 2015 WL 10786035, at *12-13 (C.D. Cal. June 23, 2015) ("self-identification through sworn statements makes sense in this case" and listing factors, including small size of individual claims).

**6. The Requirements of Rule 23(b) Are Satisfied.**

The Court has set out the applicable legal standard for predominance and superiority under Rule 23(b), which Plaintiffs adopt here. See Path App Order, at 9.

Plaintiffs focus their discussion of the predominance subject on the five issues the Court addressed in the Path App Order (a few of which will require no more than a sentence or two): choice of law, the so-called "subjective expectation of privacy" element to Plaintiffs' claim, the claim that the specific content and sharing of address book data on any user's iDevice is relevant to the intrusion claim, the supposed inclusion of "uninjured" members in the class definition(s) and the measure and calculation of classwide damages.

**a. Choice of Law.**

The Court applied California's choice of law rules to determine the controlling substantive law in the case against Apple and Path. See Path App Order, at 10 et seq. Plaintiffs adopt the Court's analysis under those rules for present purposes.

That analysis should not differ as it pertains to Apple – its "choice of law provision requires application of California law" to the aiding and abetting claims here. Path App Order, at 12. Instagram, Twitter and Yelp all appear to be similarly situated: All three are resident here, all three have what they represent are presumptively-enforceable California choice of law and choice of forum provisions in their respective Terms of Use and, in the case of Twitter and Yelp anyway, both have proffered those provisions to the Court in this case. See ECF No. 126 [Leichtling (Yelp) Decl.], at ¶ 5 et seq. & Ex. A; ECF No. 137 [Kim (Twitter) Decl.], at ¶ 8 & Ex. C et seq. Cf. ECF No. 128 [Systrom (Instagram) Decl.], at ¶ 3 et seq.; Buck Decl. at ¶ 16 & Ex. O [IG_OPP 77-78].

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

Regardless, to the extent California's three-step governmental interest test applies, the Court should still find as it did before on the Path App. See Path App Order, at 12 et seq. Under that test, Plaintiffs bear the initial burden to show California has significant contact to the claims of each class member, to satisfy constitutional due process concerns. *Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 589-90 (9th Cir. 2012).

All of the App Defendants submitted their respective apps to Apple in this District, where Apple conducts the heart of its business. Apple's review of all of the App Defendants' apps – a process that Apple has publicly characterized as "comprehensive" (see ECF 502 [Apple RJN], at ¶ 6 & Exh. F), entailing coordination between "a team of individuals responsible for conducting a review of every app to determine whether or not it may be distributed through the App Store" and the submitting companies – occurs in Santa Clara County, California (see ECF No. 147-1 [Buckley Decl.], at ¶¶ 4-5).

Apple operates its App Store, which distributes the Find Friends Versions of each of the App Defendants, from this State. See ECF No. 217 [Sparks Order], at 6. This is pursuant to an agreement that each of the App Defendants enters into with Apple, calling for application of California law and the choice of a California forum to that relationship. See ECF No. 670-1, at 21. Cf. Buck Decl. at ¶ 15, 19 & Exhs. N, R [FS_S 201; KIK_OPP 41]. On these grounds, this State is the central nexus for the putative class claims, just as Judge Sparks concluded. See ECF No. 217, at 7 ("California is the center of this type of economic activity"). Taken together, all of the above should satisfy due process considerations.

Applying the *Mazza* choice of law standard, the burden then shifts to the App Defendants (the parties opposing nationwide application of California law) to establish first, that there is a material difference in state laws on intrusion and second, that the material difference implicates specific state interests outside of this State. The Court has previously held that state law differences are material but nonetheless resolved the *Mazza* test in favor of nationwide application of California law. See Path App Order, at 16. The same resolution should obtain here.

The third step of the *Mazza* choice of law standard requires the Court to scrutinize the

comparable state interests at stake if it applies California law nationwide. Given the Path App Order, Plaintiffs anticipate Defendants will need to show "how the application of California state law would frustrate the interests of any foreign state." See Path App Order, at 15. But states outside of California would appear to have no legitimate interest in applying their laws in a manner that protects business entities from misconduct centered in California from liability outside of California when those entities (1) have agreed to be bound by California law in their contracts with Apple, and (2) offer no evidence that their digital goods or services vary on a state-by-state basis (they don't).

Even assuming that some state's materially different intrusion law manifests a genuinely-expressed interest in competing with California to attract App Store business, the App Defendants must make that business case with reference to "the facts and circumstances of *this* case." See Path App Order, at 15 (quoting *Forcellati v. Hyland's, Inc*., No. CV 12-1983-GHK MRWX, 2014 WL 1410264, at *2 (C.D. Cal. Apr. 9, 2014) (emphasis in original)). Any state interest weighed against California's interest in *this* case must account for the realities of the App Defendants' business model.

That model is "centered" (Judge Sparks' word) in the State of California, where the App Store is based. As noted, the App Defendants' products are distributed from this State via the App Store, and the App Defendants do not target their respective offerings to residents located in any particular state. No foreign state has a genuine interest in attracting more downloads from the Apple App Store; that goal directly contradicts that the App Defendants distribute the same app nationwide to users' mobile devices.

Nor can the App Defendants show that they operated in a manner in "reasonable reliance" on any specific foreign state law that they claim here would have established materially different results here. *Kearney v. Salomon Smith Barney*, 39 Cal. 4th 95, 101 (2006). As noted, each of the App Defendants (even those like Foursquare and Kik who foisted on users a choice of law provision calling for a law other than that of the State of California) entered into an agreement with Apple, calling for application of California law and the choice of a California forum in the business relationship giving rise to this case and to the distribution of their

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

respective apps by Apple to the public.

**b. Subjective Expectations of Privacy.**

The Court held that the elements under California law of an intrusion claim do "not require individualized determinations of class members' subjective expectations [of privacy]." See Path App Order, at 16-17. For the reasons given above, because California law applies to Plaintiffs' intrusion claim against the App Defendants, "the inquiry [under applicable substantive law] will be classwide, not individualized." *Id.* at 17.

**c. Phone Contents and Sharing.**

As the Court held, "Plaintiffs' claims are based on the private nature of the collection of information in an address book, not its individual components. [] Plaintiffs have a reasonable expectation of privacy in the collection of private information in their iDevice address books." See Path App Order at 18. The same analysis applies here.

**d. "Uninjured" Class Members.**

The Court rejected this Article III challenge to a class of those who "suffered from [an app's] *unconsented to* prior access to use of [address book] data." See Path App Order, at 19-20. Plaintiffs have defined each of the app classes to include only those users of a charged app who had their address book data uploaded without notice or consent. Whether the App Defendants' claimed notice and consent flow were adequate is a matter for determination by the jury. Therefore, each putative class member of each app class suffered injury from the same intrusion.

**e. Injury and Damages.**

The Court held that Plaintiffs have shown that the nominal damages claims of the proposed classes can be determined on a classwide basis, and that the availability of punitive damages for any such class is amenable to classwide resolution. See Path App Order, at 25 & 27. This holding should suffice for present purposes.

Plaintiffs reserve their right to reassert that damages for the inherent value of the classes' privacy interest invaded as well as for unjust enrichment of the App Defendants are viable and

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

amenable to classwide treatment. Ongoing merits discovery may reveal further support for this position.

Information is worth money; the rise of firms like the App Defendants trading on data would suggest so. Data is their currency, their stock-in-trade, their lifeblood. The other side of that proverbial coin is that, in the online economy, privacy has become a commodity (just as, many years ago, a species of the then-nascent right of privacy morphed into the right of publicity) – intangible, perhaps, but subject to measurement and valuation across a class of consumers.

**f. A Class Action Is Superior.**

This class action is superior to other available methods of adjudication for this case. See Path App Order, at 27.

## V. CONCLUSION

Plaintiffs respectfully submit that their class claims satisfy each of the requirements of Rule 23(a) and the requirements of Rule 23(b)(3) motion, certifying those classes, appointing Plaintiffs as Class Representatives as proposed for each of those classes and appointing Plaintiffs' Counsel as Class Counsel for each class. Plaintiffs also respectfully request that should the Court grant the instant motion, that it set a case management conference within 30 days of its Order to resolve a plan for class notice and trial of the Action.

Dated: Aug. 23, 2016

/s/ David M. Given

David M. Given
Nicholas A Carlin
PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
Tel: (415) 398-0900
Fax: (415) 398-0911

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

Michael von Loewenfeldt
James M. Wagstaffe
Frank Busch
KERR & WAGSTAFFE LLP
101 Mission Street, 18th Floor
San Francisco, CA 94105
Tel: (415) 371-8500
Fax: (415) 371-0500

*Interim Co-Lead Counsel for Plaintiffs*

Carl F. Schwenker (admitted *pro hac vice*)
LAW OFFICES OF CARL F. SCHWENKER
The Haehnel Building
1101 East 11th Street
Austin, TX 78702
Tel: (512) 480-8427
Fax: (512) 857-1294

*Plaintiffs' Liaison Counsel*

Jeff Edwards (admitted *pro hac vice*)
EDWARDS LAW
The Haehnel Building
1101 East 11th Street
Austin, TX 78702
Tel: (512) 623-7727
Fax: (512) 623-7729

Jennifer Sarnelli (SBN 242510)
GARDY & NOTIS, LLP
Tower 56
126 East 56th Street, 8th Floor
New York, NY 10022
Tel: (212) 905-0509
Fax: (212) 905-0508

*Plaintiffs' Steering Committee*

PHILLIPS, ERLEWINE, GIVEN & CARLIN, LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900