

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF TEXAS  
AUSTIN DIVISION

Marc Opperman, Rachelle King,	§	
Claire Moses, Gentry Hoffman,	§	
Steve Dean, Alicia Medlock,	§	
Alan Beueshasen, Scott Medlock,	§	
Greg Varner, Judy Long, Guili Biondi,	§	
Jason Green and Nirali Mandaywala,	§	Case No. <u>1:12-cv-00219</u>
on behalf of themselves and all	§	
others similarly situated,	§	
	§	
<i>Plaintiffs,</i>	§	
vs.	§	
	§	Class Action
Path, Inc., Twitter, Inc., Apple, Inc.,	§	
Facebook, Inc., Beluga, Inc.,	§	
Yelp! Inc., Burbn, Inc., Instagram, Inc.,	§	
Foursquare Labs, Inc., Gowalla Incorporated,	§	
Foodspotting, Inc., Hipster, Inc., LinkedIn	§	
Corporation, Rovio Mobile Oy, ZeptoLab UK	§	Jury Trial Demanded
Limited aka ZeptoLab, Chillingo Ltd.,	§	
Electronic Arts Inc., and Kik Interactive, Inc.,	§	
	§	
<i>Defendants.</i>	§	

**PLAINTIFFS' ORIGINAL CLASS ACTION COMPLAINT**

*"Don't take things that aren't yours."*

- Robert Fulghum, *All I Really Need To Know I Learned In Kindergarten*

Plaintiffs, on behalf of themselves and all others similarly situated, allege as follows:

### NATURE OF THE ACTION

1. Millions of wireless mobile device owners now keep their private address books—lists of hundreds or even thousands of personal and professional contacts—on their mobile wireless devices. These lists, which include contact names, phone numbers, physical and e-mail addresses, job titles, birthdays, and other similar personal information amassed over the owners’ lifetimes, are some of the most personal data that owners carry on their wireless mobile devices.<sup>1</sup>

2. The defendants—several of the world’s largest and most influential technology and social networking companies—have unfortunately made, distributed and sold mobile software applications (“Apps”) that, once installed on a wireless mobile device, surreptitiously harvest, upload and illegally steal the owner’s address book data without the owner’s knowledge or consent. As revealed in a recent NEW YORK TIMES report,

“The address book in smartphones -- where some of the user’s most personal data is carried— is free for app developers to take at will, often without the phone owner’s knowledge. . . . Companies that make many of the most popular smartphone apps for Apple and Android devices — Twitter, Foursquare and

---

<sup>1</sup> See Nicole Peroth and Nick Bilton, *Mobile Apps Take Data Without Permission*, NEW YORK TIMES (online ed. at [www.nytimes.com](http://www.nytimes.com) and <http://bits.blogs.nytimes.com/2012/02/15/google-and-mobile-apps-take-data-books-without-permission/> Feb. 15, 2012) (emphasis added) (“The *address book in smartphones* [is] where some of the *user’s most personal data* is carried”).

Instagram among them — routinely gather the information in personal address books on the phone and in some cases store it on their own computers.

\* \* \*

While Apple says it prohibits and rejects any app that collects or transmits users' personal data without their permission, that has not stopped some of the most popular applications for the iPhone, iPad and iPod — like Yelp, Gowalla, Hipster and Foodspotting — from taking users' contacts and transmitting it without their knowledge.”<sup>2</sup>

3. Literally billions of contacts from the address books of tens of millions of unsuspecting wireless mobile device owners have now been accessed and stolen. The surreptitious data uploads—occurring over both cellular networks and open, public wireless access nodes in homes, coffee shops, restaurants, bars, stores and businesses all across the nation—have, quite literally, turned the address book owners' wireless mobile devices into mobile radio beacons broadcasting and publicly exposing the unsuspecting device owner's address book data to the world.

4. This class action lawsuit seeks to halt and prevent these unconscionable, illegal practices, to mandate fixes to these mobile devices and Apps to prevent these invasions of users' privacy and the unauthorized access and/or transfer of unencrypted address book data, to require that all wrongfully-obtained data be permanently purged, to impose constructive trusts over the associated benefits these defendants wrongfully and unjustly realized from the stolen data, and to recover damages for the harm suffered by the Plaintiffs and millions of other unsuspecting wireless mobile device owners whose data has been stolen and whose privacy has been severely compromised.

---

<sup>2</sup> See *id.*

## PARTIES

### Plaintiffs

5. *Plaintiff Marc Opperman* ("Mr. Opperman") is an individual residing in Austin, Texas. Mr. Opperman owns and regularly uses the following wireless mobile devices: an iPhone branded mobile phone manufactured by Apple, Inc. The following defendants' Apps are installed on Mr. Opperman's identified wireless mobile device: Path, Twitter, Facebook, Instagram, LinkedIn and Angry Birds.

6. *Plaintiff Judy Long* ("Ms. Long") is an individual residing in Austin, Texas. Ms. Long owns and regularly uses the following wireless mobile devices: an iPhone. The following defendants' Apps are installed on Ms. Long's identified wireless mobile device: Path.

7. *Plaintiff Claire Moses* ("Ms. Hodgins") is an individual residing in Austin, Texas. Ms. Hodgins owns and regularly uses the following wireless mobile devices: an iPhone. The following defendants' Apps are installed on Ms. Hodgins' identified wireless mobile device: Twitter, Facebook, Yelp!, Angry Birds and Cut the Rope.

8. *Plaintiff Gentry Hoffman* ("Mr. Hoffman") is an individual residing in Austin, Texas. Mr. Hoffman owns and regularly uses the following wireless mobile devices: an iPhone. The following defendants' Apps are installed on Mr. Hoffman's identified wireless mobile device: Twitter, Instagram, Foursquare and Yelp!.

9. ***Plaintiff Steve Dean*** (“Mr. Dean”) is an individual residing in Austin, Texas. Mr. Dean owns and regularly uses the following wireless mobile devices: an iPhone. The following defendants’ Apps are installed on Mr. Dean’s identified wireless mobile device: Twitter, Facebook, Gowalla and LinkedIn.

10. ***Plaintiff Alicia Medlock*** (“Ms. Medlock”) is an individual residing in Austin, Texas. Ms. Medlock owns and regularly uses the following wireless devices: an Android branded mobile phone manufactured by Samsung that operates on Google, Inc.’s (“Google’s”) Android operating system (“Android phone”). The following defendants’ Apps are installed on Ms. Medlock’s identified wireless mobile device: Twitter, Facebook and LinkedIn.

11. ***Plaintiff Alan Beuershasen*** (“Mr. Beuershasen”) is an individual residing Austin, Texas. Mr. Berchausen owns and regularly uses the following wireless mobile devices: an iPhone. The following defendants’ Apps are installed on Mr. Berchausen’s identified wireless mobile device: Facebook, Twitter, Gowalla, Foursquare, LinkedIn and Angry Birds.

12. ***Plaintiff Scott Medlock*** (“Mr. Medlock”) is an individual residing in Austin, Texas. Mr. Medlock owns and regularly uses the following wireless mobile device: an Android branded mobile phone manufactured by Samsung that operates on Google’s Android operating system. The following defendants’ Apps are installed on Mr. Medlock’s identified wireless mobile device: Twitter and Facebook.

13. ***Plaintiff Greg Varner*** (“Mr. Varner”) is an individual residing in Austin, Texas. Mr. Varner owns and regularly uses the following wireless mobile devices: an iPhone. The following defendants’ Apps are installed on Plaintiff’s identified wireless mobile device: Twitter, Instagram, Foursquare, Gowalla, Angry Birds and Cut the Rope.

14. ***Plaintiff Rachelle King*** (“Ms. King”) is an individual residing in Austin, Texas. Ms. King owns, regularly uses and has regularly used the following wireless mobile device(s): multiple iPhones. The following defendants’ Apps or were installed on Ms. Kings’s identified wireless mobile devices: Twitter, Facebook, FoodSpotting, Hipster, Instagram, Gowalla, and Foursquare.

15. ***Plaintiff Giuli Biondi*** (“Ms. Biondi”) is an individual residing in Austin, Texas. Mr. Biondi owns and regularly uses the following wireless mobile devices: an iPhone. The following defendants’ Apps are installed on Ms. Biondi’s identified wireless mobile device: Instagram, Twitter, Facebook, Yelp!, LinkedIn and Cut the Rope.

16. ***Plaintiff Jason Green*** (“Mr. Green”) is an individual residing in Fayetteville, Arkansas. Mr. Green owns and regularly uses the following wireless mobile devices: an iPhone. The following defendants’ Apps are installed on Ms. Green’s identified wireless mobile device: Instagram, Twitter, Facebook, Kik Messenger, Path, Angry Birds and Cut the Rope.

17. *Plaintiff Nirali Mandaywala* (“Ms. Mandaywala”) is an individual residing in Austin, Texas. Mr. Mandaywala owns and regularly uses the following wireless mobile devices: an iPhone. The following defendants’ Apps are installed on Ms. Mandaywala’s identified wireless mobile device: Instagram, Twitter, Facebook, Yelp!, Gowalla, Foursquare, Angry Birds and Cut the Rope.

18. [Paragraphs 18 and 19 are intentionally left blank.]

19. [Paragraphs 18 and 19 are intentionally left blank.]

### **Defendants**

20. *Defendant Apple, Inc.* (“Apple”) is a California corporation with offices in Austin, Texas. Apple regularly conducts business in this judicial district. Apple may be served with process through its registered Texas agent, CT Corp. System, at 350 North St. Paul Street, Dallas, TX 75201-4234.

21. *Defendant Path, Inc.* (“Path”) is a Delaware corporation with its principal place of business at 400 2<sup>nd</sup> Street, Suite 350, San Francisco, California 94107. Path is not presently registered to conduct business in the State of Texas and has not designated an agent for service of process. This lawsuit arose in part out of Path’s business in this judicial district as more specifically described below. Path may be served by certified mail, return receipt requested directed to Path at its principal place of business through the Texas Secretary of State as its agent for service of process at Citations Division, 1019 Brazos, Austin, Texas 78701: 400 2<sup>nd</sup> Street, Suite 350, San Francisco, California 94107.

22. *Defendant Twitter, Inc.* ("Twitter") is a Delaware corporation with its principal place of business at 795 Folsom Street, Suite 600, San Francisco, California 94107. Twitter is not presently registered to conduct business in the State of Texas and has not designated an agent for service of process. This lawsuit arose in part out of Twitter's business in this judicial district as more specifically described below. Twitter may be served by certified mail, return receipt requested directed to Twitter at its principal place of business through the Texas Secretary of State as its agent for service of process at Citations Division, 1019 Brazos, Austin, Texas 78701: 795 Folsom Street, Suite 600, San Francisco, California 94107.

23. *Defendant Facebook, Inc.* ("Facebook") is a Delaware corporation with offices in Austin, Texas. Facebook regularly conducts business in this judicial district and this lawsuit arose in part out of Facebook's business in this judicial district as more specifically described below. Facebook may be served with process through its registered Texas agent, Corporation Service Company d/b/a CSC –Lawyers Inco, at 211 E. 7<sup>th</sup> Street, Suite 620, Austin, Texas 78701. On information and belief, Facebook has acquired the companies that formerly owned the Gowalla App (i.e., Defendant Gowalla Incorporated) and the Beluga App and/or those companies' assets and personnel and is the successor-in-interest to each of those companies.

24. *Defendant Yelp! Inc.* ("Yelp") is a Delaware corporation with its principal place of business at 706 Mission Street, San Francisco, California 94103-3162. Yelp



regularly conducts business in this judicial district and this lawsuit arose in part out of Yelp's business in this judicial district as more specifically described below. Yelp may be served with process through its registered Texas agent, National Registered Agents, Inc., at 16055 Space Center Blvd., Suite 235, Houston, Texas 77062.

25. On information and belief, *Defendant Burbn, Inc.* ("Burbn") is a Delaware corporation with its principal place of business at 265 Rivoli Street 4, San Francisco, California 94105. Burbn is not presently registered to conduct business in the State of Texas and has not designated an agent for service of process. This lawsuit arose in part out of Burbn's business in this judicial district as more specifically described below.

Burbn may be served by certified mail, return receipt requested directed to Burbn at its principal place of business through the Texas Secretary of State as its agent for service of process at Citations Division, 1019 Brazos, Austin, Texas 78701: 265 Rivoli Street 4, San Francisco, California 94105.

26. On information and belief, *Defendant Instagram, Inc.* ("Instagram") is a Delaware corporation with its principal place of business at 181 South Park Avenue, San Francisco, California 94107. On information and belief, Instagram is either a successor-in-interest to the business of Burbn or is related to or affiliated with Burbn. Instagram is not presently registered to conduct business in the State of Texas and has not designated an agent for service of process. This lawsuit arose in part out of Instagram's business in this judicial district as more specifically described below. Instagram may be

served by certified mail, return receipt requested directed to Instagram at its principal place of business through the Texas Secretary of State as its agent for service of process at Citations Division, 1019 Brazos, Austin, Texas 78701: 181 South Park Avenue, San Francisco, California 94107.

27. On information and belief, *Defendant Foursquare Labs, Inc.* (“Foursquare Labs”) is a Delaware corporation with its principal place of business at 36 Cooper Square, 6<sup>th</sup> Floor, New York, New York. Foursquare Labs is not presently registered to conduct business in the State of Texas and has not designated an agent for service of process. This lawsuit arose in part out of Foursquare Labs’s business in this judicial district as more specifically described below. Foursquare Labs may be served by certified mail, return receipt requested directed to Foursquare Labs at its principal place of business through the Texas Secretary of State as its agent for service of process at Citations Division, 1019 Brazos, Austin, Texas 78701: 36 Cooper Square, 6<sup>th</sup> Floor, New York, New York.

28. *Defendant Gowalla Incorporated* (“Gowalla”) is a Delaware corporation with its principal place of business at 610 W. 5<sup>th</sup> Street, Suite 604, Austin, Texas 78701. Gowalla regularly conducts business in this judicial district and this lawsuit arose in part out of Gowalla’s business in this judicial district as more specifically described below. Gowalla may be served with process at its principal place of business or through its registered Texas agent, National Registered Agents, Inc., at 16055 Space

Center Blvd., Suite 235, Houston, Texas 77062. On information and belief, Facebook acquired the Gowalla App and Gowalla's staff and assets in December 2011 and is the successor-in-interest to Gowalla.

29. ***Defendant Foodspotting, Inc.*** ("Foodspotting") is a Delaware corporation with its principal place of business at 526 2<sup>nd</sup> Street, San Francisco, California 94107 and its registered Delaware agent for service of process is Incorporating Services, Ltd., 3500 South DuPont Highway, Dover, Delaware 19901. Foodspotting is not presently registered to conduct business in the State of Texas and has not designated an agent for service of process in Texas. This lawsuit arose in part out of Foodspotting's business in this judicial district as more specifically described below. Foodspotting may be served by certified mail, return receipt requested directed to Foodspotting at its principal place of business through the Texas Secretary of State as its agent for service of process at Citations Division, 1019 Brazos, Austin, Texas 78701; 526 2<sup>nd</sup> Street, San Francisco, California 94107.

30. ***Defendant Hipster, Inc.*** ("Hipster") is a Delaware corporation with its principal place of business at 3130 Lowell Ave., California 90032-2913 and its registered Delaware agent for service of process is Agents and Corporations, Inc., 1201 Orange Street, Suite 600, One Commerce Center, Delaware 19801. Hipster is not presently registered to conduct business in the State of Texas and has not designated an agent for service of process in Texas. This lawsuit arose in part out of Hipster's business in this

judicial district as more specifically described below. Hipster may be served by certified mail, return receipt requested directed to Hipster at its principal place of business through the Texas Secretary of State as its agent for service of process at Citations Division, 1019 Brazos, Austin, Texas 78701: 3130 Lowell Ave., California 90032-2913.

31. *Defendant LinkedIn Corporation* (“LinkedIn”) is a Delaware corporation with its principal place of business at 2029 Stierlin Court, Mountain View, California 94043-4655 and its registered Delaware agent for service of process is Corporation Service Company, 2711 Centerville Road, Suite 400, Wilmington, Delaware 19808. LinkedIn is presently registered to conduct business in the State of Texas but has not designated an agent for service of process in Texas. This lawsuit arose in part out of LinkedIn’s business in this judicial district as more specifically described below. LinkedIn may be served by certified mail, return receipt requested directed to LinkedIn at its principal place of business through the Texas Secretary of State as its agent for service of process at Citations Division, 1019 Brazos, Austin, Texas 78701: 2029 Stierlin Court, Mountain View, California 94043-4655.

32. *Defendant Rovio Mobile Oy* (“Rovio”) is a Finland corporation with its principal place of business at Keilaranta 19 D 02150 Espoo Finland. Rovio is not registered to conduct business in the State of Texas and has not designated an agent for service of process in Texas. This lawsuit arose in part out of Rovio’s business in this

judicial district as more specifically described below. Rovio may be served by certified mail, return receipt requested directed to Rovio at its principal place of business through the Texas Secretary of State as its agent for service of process at Citations Division, 1019 Brazos, Austin, Texas 78701: Keilaranta 19 D 02150 Espoo Finland.

33. *Defendant ZeptoLab UK Limited aka ZeptoLab* ("ZeptoLab") is a United Kingdom limited company with its principal place of business at 11 Staple Inn Buildings, London, United Kingdom WC1V7QH. ZeptoLab is not presently registered to conduct business in the State of Texas and has not designated an agent for service of process in Texas. This lawsuit arose in part out of ZeptoLab's business in this judicial district as more specifically described below. ZeptoLab may be served by certified mail, return receipt requested directed to ZeptoLab at its principal place of business through the Texas Secretary of State as its agent for service of process at Citations Division, 1019 Brazos, Austin, Texas 78701: 11 Staple Inn Buildings, London, United Kingdom WC1V7QH.

34. *Defendant Chillingo Ltd.* ("Chillingo") is a United Kingdom limited company with its principal place of business at Beechfield House, Winterton Way, Macclesfield, SK 11 OLP, United Kingdom. On information and belief, Chillingo was acquired by and became a division Electronic Arts Inc. on or about October 19, 2010. Chillingo is not presently registered to conduct business in the State of Texas and has not designated an agent for service of process in Texas. This lawsuit arose in part out of

Chillingo's business in this judicial district as more specifically described below.

Chillingo may be served via Electronic Arts Inc. or by certified mail, return receipt requested directed to Chillingo at its principal place of business through the Texas Secretary of State as its agent for service of process at Citations Division, 1019 Brazos, Austin, Texas 78701: Beechfield House, Winterton Way, Macclesfield, SK 11 OLP, United Kingdom.

35. *Defendant Electronic Arts Inc.* ("Electronic Arts") is a Delaware corporation with offices in Austin, Texas. On or about October 19, 2010, Electronic Arts acquired Chillingo and, on information and belief, has since operated it as a division within Electronic Arts. As such, Electronic Arts has become Chillingo's successor-in-interest. Electronic Arts regularly conducts business in this judicial district and this lawsuit arose in part out of Electronic Arts' business in this judicial district via its Chillingo division as more specifically described below. Electronic Arts may be served with process through its registered Texas agent, National Corporate Research, Ltd., 800 Brazos, Suite 400, Austin, Texas 78701.

36. *Defendant Kik Interactive, Inc.* ("Kik Interactive") is a Canadian corporation with its principal place of business at 420 Weber St. North, Unit I, Waterloo, N2L 4E7, Canada. Kik Interactive is not presently registered to conduct business in the State of Texas and has not designated an agent for service of process in Texas. This lawsuit arose in part out of Kik Interactive's business in this judicial district as more

specifically described below. Kik Interactive may be served by certified mail, return receipt requested directed to Kik Interactive at its principal place of business through the Texas Secretary of State as its agent for service of process at Citations Division, 1019 Brazos, Austin, Texas 78701: 420 Weber St. North, Unit I, Waterloo, N2L 4E7, Canada.

37. *Defendant Beluga, Inc.* (“Beluga”) is a Delaware corporation with its principal place of business at 801 California Street, Mountain View, California 94041 and its registered Delaware agent for service of process is Incorporating Services, Ltd., 3500 South DuPont Highway, Dover, Delaware 19901. Beluga is not presently registered to conduct business in the State of Texas and has not designated an agent for service of process in Texas. This lawsuit arose in part out of Beluga’s business in this judicial district as more specifically described below. Beluga may be served by certified mail, return receipt requested directed to Beluga at its principal place of business through the Texas Secretary of State as its agent for service of process at Citations Division, 1019 Brazos, Austin, Texas 78701: 801 California Street, Mountain View, California 94041. On information and belief, Facebook acquired the Beluga App and Beluga’s staff and assets in December 2011 and is the successor-in- interest to Beluga.

38. The plaintiffs and defendants are collectively referred to herein as the “Plaintiffs” and “Defendants,” respectively. Plaintiffs anticipate the potential joinder as additional party defendants other companies who discovery or subsequently learned information reveals have made, distributed and/or sold Apps that, once installed on a

wireless mobile device, surreptitiously harvest, upload and steal the device owner's address book data without the owner's knowledge or effective consent.

### JURISDICTION AND VENUE

39. This Court has subject matter jurisdiction over this action under: (a) 28 U.S.C. § 1331 (federal question), (b) 28 U.S.C. § 1332(d) (CAFA) because (i) there are 100 or more Class Members, (ii) at least one Class Member is a citizen of a state that is diverse from any Defendant's citizenship, and (iii) the matter in controversy exceeds \$5,000,000 USD exclusive of interest and costs; (c) 18 U.S.C. § 1030(g), *et seq.* (civil actions under the Computer Fraud & Abuse Act), (d) 18 U.S.C. § 2520, *et seq.* (civil liability under the Electronic Communications Privacy Act); and (e) 18 U.S.C. § 1964 (civil actions under the Racketeer Influenced & Corrupt Organizations Act). This Court also has subject matter jurisdiction over Plaintiffs' related state law claims under 28 U.S.C. § 1367 (supplemental jurisdiction).

40. This Court has personal jurisdiction over the Defendants because at all relevant times, each Defendant conducted (and many continue to conduct) substantial business in the Western District of Texas. Gowalla has its principal place of business and registered office in this judicial district and is thus subject to this Court's jurisdiction. Each of the remaining defendants have transacted business within this judicial district and have had sufficient minimum contacts with the State of Texas and this judicial district so that they are amenable to service of process under the Texas



long-arm statute (TEX. CIV. PRAC. & REM. CODE §§ 17.041-.045) and FED. R. CIV. P. Rule 4(e) and so that requiring the Defendants to respond to this action would not violate due process.

41. Venue is proper in the Western District of Texas under 28 U.S.C. § 1391(b) and (c) because, as described herein, (i) both Plaintiffs and defendant Gowalla reside within this judicial district, (ii) each defendant conducts substantial business in this judicial district, (iii) defendants Apple, Electronic Arts, Gowalla and Facebook have offices, personnel and operations within this judicial district, (iv) a substantial part of the events or omissions giving rise to these claims occurred within this judicial district, and (v) a substantial part of the personal property that is the subject of this action—i.e., the wireless mobile devices and the owners’ personal address book data contained on their wireless mobile devices—is situated within this judicial district.

#### NATURE OF THE CLAIMS

42. This is a class action lawsuit brought by Plaintiffs on behalf of themselves and all other similarly situated persons (*i.e.*, the “Class members”) whose privacy was invaded and whose personal address book data (including contact names, phone numbers, physical and e-mail addresses, job titles, birthdays, etc.) that had been communicated to and/or maintained on their wireless mobile devices was surreptitiously accessed, harvested uploaded and/or broadcast from their wireless mobile devices and used without their knowledge or permission by means of Apps and

products made, distributed, authorized, approved and/or sold by the defendant companies named in this lawsuit. This is an action for injunctive relief, equitable relief and damages.

43. As described herein, Plaintiffs and the putative Class members seek injunctive, equitable, statutory and monetary relief for, *inter alia*, invasion of privacy, violations of TEX. PENAL CODE §§ 16.02(b) (intentional interception, disclosure or use of wire or electronic communication), 31.03 (consolidated theft offenses) and 33.02 (breach of computer security), negligence, common law misappropriation, theft under the Theft Liability Act (TEX. CIV. PRAC. & REM. CODE ANN. §134.001, *et seq.*), civil liability under the Texas Wiretapping Act for intentional interception, disclosure or use of wire or electronic communications (TEX. CODE CRIM. PROC. Art. 18.20, §16(a)), conversion, unjust enrichment, theft of Plaintiffs' private information and unlawful interception of, access to, broadcast and use and transmission in interstate commerce of Plaintiffs' data and electronic communications in violation of the Electronic Communication Privacy Act (18 U.S.C. § 2701, *et seq.*), the Computer Fraud and Abuse Act (18 U.S.C. § 1030(g)) and common law, and violations of the Racketeer Influenced & Corrupt Organizations Act (including under 18 U.S.C. §§ 1343 (wire fraud), 1961 - 1964 (civil liability for racketeering activities and conspiracies), and 2314 (transportation of stolen property)) and such other state laws protecting individuals' privacy or prohibiting the

unauthorized access and/or use of others' communications, computers or data.<sup>3</sup>

Plaintiffs also seek the imposition of a constructive trust over any benefits received by the Defendants attributable to the wrongful taking, possession, access, interception, transfer, or use of the Plaintiffs' and the Class members' wireless mobile devices, address book data, private information or communications and the disgorgement of any such benefits that Defendants received.

44. Plaintiffs, on behalf of themselves and the Class members, seek (i) actual damages, economic damages, statutory and treble damages and/or nominal damages, (ii) exemplary damages as authorized by statute, (iii) injunctive and equitable relief, and (iv) attorneys' fees, litigation expenses and costs of suit.

45. All causes of action are based on the same operative facts.

#### **CLASS ACTION ALLEGATIONS**

46. Plaintiffs bring this action as a class action under Rules 23(a), 23(b)(1), 23(b)(2) and 23(b)(3) of the Federal Rules of Civil Procedure on behalf of a Class of similarly situated persons consisting of:

---

<sup>3</sup> See also CAL. CONST. ART. I, SEC. 1 ("*All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."*) (emphasis added); CAL. PENAL CODE § 502 (proving criminal and civil liability for accessing or using of others' computers or data without proper permissions); CAL. CIV. CODE §§ 22575 - 22579 (California Online Privacy Protection Act); CAL. PENAL CODE § 637 (imposing civil liability for violations of CAL. PENAL CODE § 631 (the California Wiretap Act) and CAL. PENAL CODE § 632 (the California Eavesdropping and Confidential Communication statute)); *Kremen v. Cohen*, 337 F.3d 1024 (9<sup>th</sup> Cir. 2003) (upholding claims for conversion of intangible property).

Plaintiffs and all owners of iOS- or Android-based wireless mobile devices who acquired from Apple's AppStore, Google's Android Market, Amazon.com's Appstore for Android any App that without the owner's prior effective consent accessed, copied, uploaded, transferred, broadcast and/or otherwise used any portion of the owner's address book data (including, for example, contact names, phone numbers, physical or e-mail addresses, job titles, birthdays, etc.) that the owner had transferred onto the owner's wireless mobile device, specifically including any of the following Apps: Path, Twitter, Facebook, Instagram, Foursquare, Gowalla, Beluga, Foodspotting, Yelp!, Hipster, Kik Messenger, LinkedIn, Angry Birds, or Cut the Rope and other unknown Apps having similar address book data harvesting functionalities, (the "Class") and were damaged thereby.

Excluded from the Class are the Defendants and their officers, directors, managing agents and subsidiaries, members of Defendants' immediate families, the Court and any Court personnel, and the legal representatives, heirs, successors or assigns of any excluded person or entity.

47. Numerosity: The Class is so numerous that joinder of all members is impracticable. The precise number of Class members can only be ascertained through appropriate discovery from the Defendants. However, based on the widespread consumer adoption of iOS- and Android-based wireless mobile devices and the reported multi-million-person installation base for the offending Apps described in this Complaint, Plaintiffs estimate that the putative Class is comprised of in excess of five million persons, making joinder impracticable. Accordingly, disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

48. Typicality: The named Plaintiffs' claims are typical of the claims of the members of the Class as all members of the Class are similarly affected by the Defendants' wrongful conduct in violation of the federal and state laws that are complained of herein. Indeed, the rights of each Class member were violated in a virtually identical manner—i.e., each member's wireless mobile device and the private, personal address book data maintained on his or her wireless mobile device was accessed, transferred and used in violation of numerous federal and state criminal and civil laws—as a result of the Defendants' actions and/or inactions.

49. Commonality: Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members of the Class. Among the questions of law and fact common to the Class are:

- whether it was illegal for the defendants to access, upload and/or use a wireless mobile device owner's private, personal address book data maintained on his or her wireless mobile device without the owner's permission or effective consent;
- the commercial market value of contact data points and data fields typical of those contained in Class members' address books maintained on wireless mobile devices and the technical methods used by and benefits realized by Defendants who have gleaned such address book information from Class members' wireless mobile devices;
- what criminal and civil laws were violated and what injunctive or declaratory relief or statutory, actual and other damages arise and are awardable when an App developer accesses, uploads, uses and/or broadcasts any portion of a wireless mobile device owner's private, personal address book data maintained on his or her wireless mobile device without the owner's permission or effective consent;

- whether the Defendants' acts alleged herein violated the Electronic Communication Privacy Act, the Computer Fraud and Abuse Act, the Racketeer Influenced & Corrupt Organizations Act and/or similar state and federal laws prohibiting intentional interception, disclosure or use of wire or electronic communications, theft and transportation of stolen property, breach of computer security, fraud and related activity in connection with computers, racketeering activities, common law misappropriation, conversion, invasion of privacy or unjust enrichment;
- a digital distribution App platform provider's direct, independent and/or joint and several responsibility and liability for products and services promoted on, offered over, and distributed by its digital distribution App platform service and (supposedly) tested and pre-cleared by that provider under policies that should have prevented a non-complaint, Trojan-horse like App—here, ones that expose and facilitate the theft of the wireless mobile device owner's private address book data and information—from reaching the market or being available to the Class members;
- whether Defendants acted knowingly, intentionally, maliciously, wantonly or recklessly in creating and/or distributing to the market the Apps in suit (and other similarly functioning Apps) and in accessing and using the Class members' wireless mobile device's private, personal address book data without permission or effective consent; and,
- whether the members of the Class have sustained compensable or statutory damages and, if so, the proper measure of damages.

50. The named Plaintiffs and their counsel will fairly and adequately represent the interests of the Class. Plaintiffs have no interests that are contrary to or in conflict with those of the Class members. Plaintiffs' retained counsel have demonstrated competence in identifying recoverable Class claims and are sufficiently competent and experienced with the prosecution of cases before this Court and in this judicial district, including complex small and large scale disputes involving technology, privacy and civil rights, misappropriation of data and information, and electronic

piracy and RICO violations and have worked and served as counsel on both federal and state class action matters.

51. Plaintiffs know of no difficulties that will be encountered in the management of this action that would preclude its maintenance as a class action, either with or without sub-classes.

52. A class action is superior to other available methods for fairly and efficiently adjudicating this controversy, especially since joinder of all members is impracticable. Plaintiffs and the Class members have been irreparably harmed as a result of the Defendants' wrongful actions and/or inactions. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Defendants' conduct.

52. Furthermore, as the damages suffered by individual Class members may be proportionately small, the expense and burden of individual litigations make it virtually impossible on a cost-effective basis for members of the Class to individually redress the unlawful conduct alleged and wrongs done to them. That burden would substantially impair the ability of Class members to pursue individual lawsuits in order to vindicate their rights. Consequently, absent a class action, Defendants would retain the benefits of their wrongdoing despite the serious nature of their violations of the law.

53. Accordingly, class certification is appropriate under Rule 23.

## BACKGROUND – WIRELESS MOBILE DEVICES AND THE APP MARKET

54. Generally speaking, wireless mobile devices are a class of hand-held, internet-enabled computers that also double as communication devices, such as smartphones and tablet computers. These devices ordinarily operate over a wireless and/or cell phone voice-data network and the operating systems for these devices typically contain an Application Programming Interface (“API”) that enables the devices to run third-party developed mobile software applications, commonly called “Apps.” Apps are available through application distribution platforms, which are typically operated by the owner of the operating system, and are ordinarily loaded directly to the target wireless mobile device (though they can occasionally be loaded to laptops or desktops first for subsequent installation on the wireless mobile device).<sup>4</sup>

55. Partially as result of these features, demand for wireless mobile communication devices (especially smartphones and tablet computers) and the Apps that run on them has grown tremendously in recent years and a lucrative industry has sprung up designing and selling Apps for various mobile wireless devices. Consumers have now purchased hundreds of millions of wireless mobile devices and have downloaded tens of billions of Apps through Apple’s AppStore, Google’s Android Marketplace and Amazon.com, Inc.’s (“Amazon.com”) Android Marketplace. Indeed,

---

<sup>4</sup> See, e.g., MG Siegler, *Analyst: There’s a great future in iPhone apps*, VENTURE BEAT (June 11, 2008) at <http://venturebeat.com/2008/06/11/analyst-theres-a-great-future-in-iphone-apps/>.



as of the fourth quarter of 2011, approximately 46% of Americans owned some sort of smartphone.<sup>5</sup>

**APPLE AND GOOGLE DOMINATE THE MARKET FOR WIRELESS MOBILE DEVICE AND APPS**

56. Apple and Google developed and own the two dominant mobile operating systems for wireless mobile devices (with Blackberry, Microsoft and a few other players holding a smaller market share).<sup>6</sup> Apple also manufactures and sells the following wireless mobile devices: the iPhone, the iPad and the iPod Touch. As of December 31, 2011, Apple had sold approximately 183,078,000 iPhones, 55,280,000 iPads and 60,000,000 iPod Touches.<sup>7</sup>

57. Apple's iOS mobile operating system is deployed on Apple's own line of Apple-manufactured iPhones, iPads and iPod Touches. Google's Android mobile operating system is an open-source platform backed by Google and is deployed on a variety of third-party manufactured smartphones and tablet devices. Approximately 36.3 million Android phones were sold in first quarter of 2011 alone.

---

<sup>5</sup> See *More US Consumers Choosing Smartphones as Apple Closes the Gap on Android*, NIELSENWIRE (January 18, 2012) at <http://blog.nielsen.com/nielsenwire/consumer/more-us-consumers-choosing-smartphones-as-apple-closes-the-gap-on-android/> ("As of Q42011, 46 percent of US mobile consumers had smartphones, and that figure is growing quickly. In fact, 60 percent of those who said they got a new device within the last three months chose a smartphone over a feature phone.").

<sup>6</sup> See *id.*

<sup>7</sup> See Apple, Inc.'s Quarterly and Annual Financial Reports, as filed with the U.S. Securities and Exchange Commission.

58. In the United States, as of late 2011 Google's Android platform was deployed on approximate 47.3% of smartphones while Apple's iOS operating system is installed on approximately 29.6% of smartphones.

59. Both Apple and Google have also created, own and operate their own digital App distribution platforms where they both make available hundreds of thousands of self-developed and third-party Apps compatible with wireless mobile devices running their respective mobile operating systems.

60. Google's digital distribution platform, which opened and went live in October of 2008, is called the "Android Market." As of January 2012, Android phone owners had downloaded over 10 billion Apps from the Android Market, which now has over 400,000 Apps available.<sup>8</sup>

#### **Apple's App Store and its Mobile App Arrangements with App Developers**

62. Apple's digital distribution platform, which opened and went live on approximately July 10, 2008, is called the "App Store."<sup>9</sup> As of June 6, 2011, 425,000 third-party Apps were available for distribution to 200 million iOS device users. During the first week of March 2012, Apple announced its 25 billionth App download. Apple's App store is the exclusive source for Apple and third-party developed Apps designed to run on Apple's iPhone, iPad and iPod Touch mobile wireless devices.

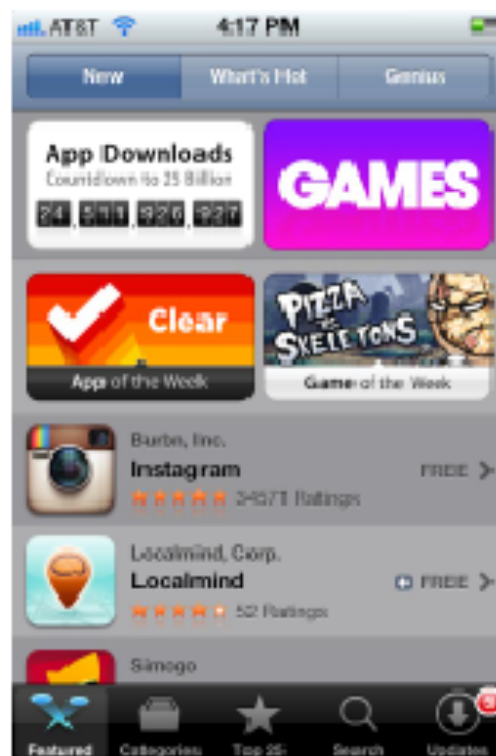
---

<sup>8</sup> See Barra, Hugo, "Android: momentum, mobile and more at Google I/O", THE OFFICIAL GOOGLE BLOG (May 10, 2011) at <http://googleblog.blogspot.com/2011/05/android-momentum-mobile-and-more-at.html>.

<sup>9</sup> See *10 Billion App Countdown* (Apple release Jan. 14, 2011) at <http://www.apple.com/itunes/10-billion-app-countdown/>.

63. Apple also pre-installs various Apple-developed, standard Apps on its iPhones, iPads and iPod Touches that are integrated into its iOS mobile operating system, including an App called “Contacts” for storing the owner’s address book data (including contact names, phone numbers, physical and e-mail addresses, job titles, birthdays, and other similar private, personal information) and an App entitled “App Store” that links to the mobile version of Apple’s App Store and enables mobile App Store functionality on the owners’ wireless mobile devices. A sample screen shot of an iPhone displaying the App Store resident on the iPhone (and listing and promoting the availability of the Instagram App) is shown in Figure 1 immediately below:

Fig. 1. iPhone AppStore sample screen shot.



64. Apple has designed its iPhone, iPad and iPod Touch wireless mobile devices to accept Apps only from Apple's AppStore, making Apple's AppStore essentially the exclusive source from which consumers may obtain Apps for their iPhone, iPad and iPod Touch wireless mobile devices (with the exception "jailbroken" devices that are modified to circumvent the iOS operating system's downloading restrictions).<sup>10</sup>

65. Apple is reported to have captured 99.4% of the 4.5 billion sales of mobile apps in 2009 (with associated gross App revenues of \$6.8 Billion).<sup>11</sup> Articles estimate that by 2013, total mobile app revenues will reach a staggering \$29.5 billion. Apple's AppStore had \$1.782 billion in revenues in 2010 and in excess of \$4 billion in revenues in 2011. As of March 2012, approximately 25 billion Apps have been downloaded via Apple's App Store.<sup>12</sup>

66. To gain entry into the incredibly lucrative iPhone, iPod Touch and iPad App market, aspiring App developers must first partner with Apple. Specifically,

---

<sup>10</sup> See Walter Isaacson, STEVE JOBS at p. 501 (Simon & Schuster, Oct. 24, 2011) ("[Apple CEO Steve] Jobs soon figured out that there was a way to have the best of both worlds. He would permit outsiders to write apps, but they would have to meet **strict standards, be tested and approved by Apple, and be sold only through the iTunes Store**. It was a way to reap the advantage of empowering thousands of software developers while **retaining** enough **control** to protect the integrity of the iPhone and the simplicity of the customer experience. 'It was an absolute magical solution that hit the sweet spot,' said [Apple board member Arthur D.] Levinson. 'It gave us the benefit of openness while retaining **end-to-end control**.'" (emphasis added).

<sup>11</sup> See <http://arstechnica.com/apple/news/2010/01/apple-responsible-for-994-of-mobile-app-sales-in-2009.ars>.

<sup>12</sup> See, e.g., Apple Press Release at [www.apple.com/about/job-creation/](http://www.apple.com/about/job-creation/) (boasting that Apple's AppStore has had "more than 550,000 apps and more than 24 billion downloads in less than four years").

Apple requires developers to pay Apple a \$99 yearly registration fee<sup>13</sup> and agree to and execute Apple's standard-form iPhone Developer Program License Agreement ("IDPLA"). Among other things, the IDPLA serves as a license agreement, authorizing developers to utilize proprietary Apple software to build iPhone, iPod Touch and iPad Apps. Together, the Apple software and registered App developer program provides access to a wealth of information, tools, diagnostics and technical support services that Apple specifically designed to facilitate the development of applications for Apple's products. These valuable resources include editing software, simulators, forums, code, code resources and libraries, performance enhancing tools, testing software and access to a cadre of Apple engineers who "provide ... code-level assistance, helpful guidance, [and] point [the developer] towards the appropriate technical documentation to fast-track [his/her] development process."<sup>14</sup> In short, it is effectively impossible to develop an iPhone, iPad or iPod Touch App without Apple's consent, software and material assistance; but once registered and licensed, App developers are provided virtually all of the tools, information and technical assistance needed to create an App for the iPhone, iPad or iPod Touch.

67. Notwithstanding, there is no guarantee that an iOS App will actually go to market. To the contrary, Apple maintains strict and uniform control over the

---

<sup>13</sup> See Apple iOS Developer Program Registration and Information Webpage at <https://developer.apple.com/programs/ios/>.

<sup>14</sup> See Apple iOS Developer Program "Develop" and "Test" Webpages at <http://developer.apple.com/programs/ios/develop.html> and <http://developer.apple.com/programs/ios/test.html>.

“selection” of Apps it deems worthy, and provides the sole and exclusive storefront for those sales through its AppStore. In other words, in addition to acting as “facilitator,” Apple also acts as “gatekeeper.”

68. For example, Apple has rejected Apps for competitive reasons—such as if the third-party App duplicates an Apple App—and occasionally even for moral reasons, with Apple’s CEO Steve Jobs having notably said, “We do believe we have a moral responsibility to keep porn off the iPhone . . . Folks who want porn can buy an Android phone.”<sup>15</sup>

69. Mr. Jobs further expressed that Apple’s control over the approval of Apps for iOS-system devices was instituted, in part, to provide device owners “**freedom from programs that steal your private data** [and] freedom from programs that trash your battery.”<sup>16</sup>

70. To get applications into the AppStore, Apple requires developers to submit their App and wait for approval or rejection by Apple (and rejected Apps are given feedback on the reason they were rejected so they can be modified and

---

<sup>15</sup> Apple E-mail from Apple CEO Steve Jobs to Matthew Browning (April 2010); Walter Isaacson, STEVE JOBS at p. 516 (Simon & Schuster, Oct. 24, 2011).

<sup>16</sup> Apple E-mail from Apple CEO Steve Jobs to Valleywag website editor Ryan Tate (May 2010) copied at <http://venturebeat.com/2010/05/15/steve-jobs-to-valleywag-why-are-you-so-bitter/> (emphasis added); Walter Isaacson, STEVE JOBS at p. 516 (Simon & Schuster, Oct. 24, 2011).

resubmitted).<sup>17</sup> Apple describes the purpose of the approval and verification process as follows:

“The app approval process is in place to ensure that applications are reliable, perform as expected, and are free of explicit and offensive material. **We review every app on the App Store based on a set of technical, content, and design criteria.** . . . These guidelines are designed to help you prepare your iOS and Mac OS X apps for the approval process.”<sup>18</sup>

71. In fact, since 2010, Apple's own AppStore Guidelines (available to both developers and the public) have **explicitly forbidden** Apps having the following functionalities:

“17.1: 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

17.2: Apps that require users to share personal information, such as email address and date of birth, in order to function will be rejected”

72. Similarly, Apple, Inc.’s iPhone SDK Agreement (rev. dated 10-20-08),<sup>19</sup> which on information and belief Apple purportedly required iOS App developers to agree to and abide by, also provided as follows:

### **3.2 Use of the SDK**

As a condition to using the SDK, You agree that:

(a) You will only use the SDK for the purposes and in the manner expressly permitted by this Agreement and in accordance with all applicable laws and regulations;

---

<sup>17</sup> See, e.g., *Thoughts on the iPhone App Review Process* at <http://www.tuaw.com/2008/08/07/thoughts-on-the-iphone-app-store-review-process/>.

<sup>18</sup> Apple’s App Store Guidelines website at <https://developer.apple.com/appstore/guidelines.html> (emphasis added).

<sup>19</sup> The “SDK” abbreviation is short for “Software Development Kit.”

(b) You will not use the SDK for any unlawful or illegal activity, nor to develop any Application which would commit or facilitate the commission of a crime, or other tortious, unlawful, or illegal act;

(c) Your Application will be developed in compliance with the Documentation and the Program Requirements, the current set of which is set forth in Section 3.3 below;

(d) To the best of Your knowledge and belief, Your Application does not and will not violate, misappropriate, or infringe any copyright, patent, trademark, trade secret, rights of privacy and publicity, or other proprietary or legal right of any third party or of Apple; and

(e) You will not, through use of the SDK or otherwise, create any Application or other program that would disable, hack or otherwise interfere with any security, digital signing, digital rights management, content protection, verification or authentication mechanisms implemented in or by the iPhone operating system software, iPod touch operating system software, this SDK, or other Apple software, services or technology, or enable others to do so.

### 3.3 Program Requirements for Applications

Any Application developed using this SDK must comply with these criteria and requirements, as they may be modified by Apple from time to time:

\*

\*

\*

#### **User Interface and Data:**

3.3.5 Applications must comply with the Human Interface Guidelines and other Documentation provided by Apple.

3.3.6 Any form of user or device data collection, or image, picture or voice capture or recording performed by the **Application** (collectively “Recordings”), and any form of user data, content or information processing, maintenance, uploading, syncing, or transmission performed by the Application (collectively “Transmissions”) **must comply with all applicable privacy laws and regulations as well as any Apple program requirements related to such aspects, including but not limited to any notice or consent requirements.** In particular, a reasonably conspicuous visual indicator must be displayed to the user as part of the Application to indicate that a Recording is taking place.

#### **Location Services and User Privacy:**

3.3.7 For Applications that use location-based APIs or that collect, transmit, maintain, process, share, disclose or otherwise use a user's personal information:

- **You and the Application must comply with all applicable privacy and data collection laws and regulations** with respect to any collection, transmission, maintenance, processing, use, etc. of the user's location data or personal information by the Application.

- Applications may not be designed or marketed for the purpose of harassing, abusing, stalking, threatening or otherwise violating the legal rights (such as the rights of privacy and publicity) of others.

- For Applications that use location-based APIs, such Applications may not be designed or marketed for real time route guidance; automatic or autonomous



control of vehicles, aircraft, or other mechanical devices; dispatch or fleet management; or emergency or life-saving purposes.

- Applications may not use any robot, spider, site search or other retrieval application or device to scrape, retrieve or index services provided by Apple or its licensors, or to collect information about users for any unauthorized purpose.

3.3.8 Applications that offer location-based services or functionality must notify and obtain consent from an individual before his or her location data is being collected, transmitted or otherwise used by the Application.<sup>20</sup>

73. Nevertheless, as discussed below, Apple repeatedly permitted and even facilitated distribution over its AppStore of Apps having these exact forbidden functionalities, resulting in Apps having these forbidden functionalities being installed on and operating on millions of iOS-based wireless mobile devices.

74. For example, Apple's own IOS DEVELOPER LIBRARY publishes and provides to App developers on Apple's own web pages<sup>21</sup> html and pdf versions of a tutorial entitled *Address Book Programming Guide for iOS* containing specific instructions and

---

<sup>20</sup> Apple iPhone SDK Agreement (rev. dated 10-20-08).

<sup>21</sup> Apple's *Address Book Programming Guide for iOS* located on Apple's online IOS DEVELOPER LIBRARY at <https://developer.apple.com/library/ios/#DOCUMENTATION/ContactData/Conceptual/AddressBookProgrammingGuideforiPhone/Introduction.html> (html version) and at <https://developer.apple.com/library/ios/documentation/ContactData/Conceptual/AddressBookProgrammingGuideforiPhone/AddressBookProgrammingGuideforiPhone.pdf> (pdf version). Apple states that its iOS "Address Book framework provides access to a centralized contacts database, called the Address Book database, that stores a user's contacts. Applications such as Mail and Messages use this database to present information about known and unknown persons." *Address Book Framework Reference for iOS* at [https://developer.apple.com/library/ios/#DOCUMENTATION/AddressBook/Reference/AddressBook\\_iPhoneOS\\_Framework/index.html#apple\\_ref/doc/uid/TP40007212](https://developer.apple.com/library/ios/#DOCUMENTATION/AddressBook/Reference/AddressBook_iPhoneOS_Framework/index.html#apple_ref/doc/uid/TP40007212). Apple similarly provides explicit instructions and code for accessing and manipulating the wireless mobile device's address book data. See, e.g., *id.*

code for “programmatically accessing” the wireless mobile device’s address book data and “to interact with the Address Book directly.”<sup>22</sup>

75. A true and correct copy of the pdf version of Apple’s *Address Book Programming Guide for iOS* is attached as Exhibit 1. Notably, at page 25 **Apple specifically acknowledges and states that “the Address Book database is ultimately owned by the user.”** *Id.* (emphasis added). Nevertheless, Apple’s tutorials and developer sites also teach App developers how to code and create Apps that access, manipulate, alter, use and upload a wireless mobile device user’s address book data stored on his or her wireless mobile device.<sup>23</sup>

76. On information and belief, the code written, provided, and approved by Apple and published on Apple’s own iOS DEVELOPER LIBRARY enables Apps

---

<sup>22</sup> See APPLE iOS DEVELOPER LIBRARY *Address Book Programming Guide for iOS* websites located at <https://developer.apple.com/library/ios/#DOCUMENTATION/ContactData/Conceptual/AddressBookProgrammingGuideforiPhone/Introduction.html> , [https://developer.apple.com/library/ios/#DOCUMENTATION/ContactData/Conceptual/AddressBookProgrammingGuideforiPhone/Chapters/QuickStart.html#//apple\\_ref/doc/uid/TP40007744-CH2-SW1](https://developer.apple.com/library/ios/#DOCUMENTATION/ContactData/Conceptual/AddressBookProgrammingGuideforiPhone/Chapters/QuickStart.html#//apple_ref/doc/uid/TP40007744-CH2-SW1) , [https://developer.apple.com/library/ios/#DOCUMENTATION/ContactData/Conceptual/AddressBookProgrammingGuideforiPhone/Chapters/BasicObjects.html#//apple\\_ref/doc/uid/TP40007744-CH3-SW1](https://developer.apple.com/library/ios/#DOCUMENTATION/ContactData/Conceptual/AddressBookProgrammingGuideforiPhone/Chapters/BasicObjects.html#//apple_ref/doc/uid/TP40007744-CH3-SW1) , [https://developer.apple.com/library/ios/#DOCUMENTATION/ContactData/Conceptual/AddressBookProgrammingGuideforiPhone/Chapters/UI\\_Controllers.html#//apple\\_ref/doc/uid/TP40007744-CH5-SW1](https://developer.apple.com/library/ios/#DOCUMENTATION/ContactData/Conceptual/AddressBookProgrammingGuideforiPhone/Chapters/UI_Controllers.html#//apple_ref/doc/uid/TP40007744-CH5-SW1) , [https://developer.apple.com/library/ios/#DOCUMENTATION/ContactData/Conceptual/AddressBookProgrammingGuideforiPhone/Chapters/DirectInteraction.html#//apple\\_ref/doc/uid/TP40007744-CH6-SW1](https://developer.apple.com/library/ios/#DOCUMENTATION/ContactData/Conceptual/AddressBookProgrammingGuideforiPhone/Chapters/DirectInteraction.html#//apple_ref/doc/uid/TP40007744-CH6-SW1) , and [https://developer.apple.com/library/ios/#DOCUMENTATION/ContactData/Conceptual/AddressBookProgrammingGuideforiPhone/RevisionHistory.html#//apple\\_ref/doc/uid/TP40007744-CH999-SW1](https://developer.apple.com/library/ios/#DOCUMENTATION/ContactData/Conceptual/AddressBookProgrammingGuideforiPhone/RevisionHistory.html#//apple_ref/doc/uid/TP40007744-CH999-SW1)

<sup>23</sup> See generally Exhibit 1 and at p. 5 (“Direct Interaction: Programmatically Accessing the Database” (page 25) describes the ways your application can read and write contact information directly.”); *Address Book Framework Reference for iOS* in the APPLE iOS DEVELOPER LIBRARY at [https://developer.apple.com/library/ios/#DOCUMENTATION/AddressBook/Reference/AddressBook\\_iPhoneOS\\_Framework/\\_index.html#//apple\\_ref/doc/uid/TP40007212](https://developer.apple.com/library/ios/#DOCUMENTATION/AddressBook/Reference/AddressBook_iPhoneOS_Framework/_index.html#//apple_ref/doc/uid/TP40007212).

incorporating that code to surreptitiously access, use and upload users' wireless mobile device address book data.

77. Thus, despite supposedly mandating that App developers not include supposedly forbidden address book data harvesting functionalities into their Apps, Apple actually instead teaches App developers precisely how to incorporate forbidden address book data harvesting functionalities into their Apps, which both Apple and the App developer then distribute through Apple's AppStore for deployment on customers' iPhones, iPads and iPods, presumably to each others' immense profit.

78. On information and belief, use of this Apple-generated coding has resulted in the creation and distribution of myriad Trojan-horse like Apps—*i.e.*, Apps marketed to do one thing (for example, play Angry Birds or post and trade photos on Path) but in reality have the stealth functionality of surreptitiously harvesting a user's address book data.

79. According to a February 15, 2012 report in the NEW YORK TIMES entitled *Mobile Apps Take Data Without Permission*, a February 2011 study found that 11% of the free Apps in Apple's iTunes Store had the ability to access users' contacts.

80. On information and belief, despite Apple's written policies and agreements and public representations to the contrary, Apple's AppStore has made available for download (and has downloaded to consumers' wireless mobile devices) in excess of 100 discrete Apps containing code that functions to access, copy and upload to

remote systems at least a portion of a user's wireless mobile device's address book data without the user's express prior effective consent. Released Apps having these forbidden functionalities include those of the defendants identified herein as well as, on information and belief, those of other App development companies (the "Unknown App Developers") whose Apps—despite having similar stealth address book data harvesting functionalities—were nevertheless approved by Apple and released by Apple on its AppStore.

81. Once reviewed, validated, approved and "selected" for distribution, Apple markets, distributes and sells the developer's App through its AppStore - collecting all gross revenues and retaining 30% of such revenues for itself (and collecting additional future revenues from Apps that incorporate Apple's iAd advertising program).<sup>24</sup> Apple charges App developers no additional fees for marketing, hosting or credit card transaction fees.<sup>25</sup>

82. Even after an App reaches the market, Apple maintains ironclad control – requiring each App developer to re-submit his or her App whenever a change, update or new version is created. In addition, Apple retains (and has exercised on multiple prior occasions) the authority to terminate sales or distribution of any App and/or

---

<sup>24</sup> <http://developer.apple.com/programs/ios/distribute.html>.

<sup>25</sup> *Id.*

terminate the account of any App developer - for a variety of reasons, including non-compliance with development policies.

83. Apple touts to the market and to its iPhone, iPad and iPod Touch customers the security and peace of mind associated with Apple's prior vetting of the Apps available from its App Store. In promoting its iPhone, iPad and iPod Touch wireless mobile devices and its integrated AppStore service, Apple has publicly touted to consumers Apple's supposedly highly controlled, closed-end system and its App validation process over that of competitive Android-based wireless mobile devices.

84. In February 2012, Apple stated to press outlets in response to privacy concerns regarding App address book data harvesting issues that Apps which surreptitiously harvest and upload a user's address book data without the user's prior consent violate Apple's developer agreements.

85. Nonetheless, on information and belief, Apple has not removed any of the Defendants' offending Apps complained of herein from Apple's AppStore, terminated or suspended any of the Defendants' AppStore accounts, remotely disabled any Defendant's App, or offered its customers compensation for essentially assisting these companies with stealing their App users' private data (nor has Apple taken any such actions with regard to the Unknown App Developers).

### Google's "Android Market" App marketplace

86. Unlike Apple, Google does not currently manufacture its own line of wireless mobile devices. Instead, it licenses its Android operating system to third-party wireless mobile device manufacturers, who also ordinarily pre-install a number of Google-developed Apps and software on the wireless mobile devices.

87. Google does, however, own and operate the "Android Market," a digital distribution system and service for the sale and distribution of Google- and third-party-developed Apps designed for wireless mobile devices running Google's Android operating system.<sup>26</sup> On information and belief, an Android Market App and an App for storing the owner's address book data (including contact names, phone numbers, physical and e-mail addresses, job titles, birthdays and other similar private information) also comes pre-installed on Android phones and wireless mobile devices.

88. On information and belief, as of January 2012, approximately 10 billion Apps had been downloaded from the Android Market<sup>27</sup> and 400,000 unique Apps were available for sale/download from the Android Market.<sup>28</sup>

89. Google's Android Market is not the exclusive source for Apps for Android phones or wireless mobile tablet computers. Google nevertheless maintains a rigorous

---

<sup>26</sup> See Google's Android Market at <https://market.android.com/apps> .

<sup>27</sup> See Ronald Jacobs, *Android Market surpassed 10 billion downloads*, TECHNOFIERCE (Dec. 6, 2011) at <http://www.technofierce.com/2011/12/06/android-market-surpassed-10-billion-downloads-and-discounted-apps-offering/news/001780>.

<sup>28</sup> See Android Market webpage at <https://market.android.com/apps>.

approval and validation process for Apps published and distributed over its Android Market and places restrictions on the types of Apps that can be published, sold or distributed over its Android Market. Google maintains the right to remove (and has removed) Apps from its Android Market for violations of its Android Developer Distribution Agreement.

90. Google's Android Market Developer Program Policies, which are available at <http://www.android.com/us/developer-content-policy.html>, specifically provide as follows:

**Content Policies** Our content policies apply to any content your application displays or links to, including any ads it shows to users and any user-generated content it hosts or links to. . . . **Illegal Activities:** Keep it legal. Don't engage in unlawful activities on this product.

91. Google's Android Market Developer Distribution Agreement, which is available at <http://www.android.com/us/developer-distribution-agreement.html> and excerpted below, specifically provides as follows:

4.3 You agree that if you use the Market to distribute Products, **you will protect the privacy and legal rights of users.** If the users provide you with, or your Product accesses or uses, user names, passwords, or other login information or personal information, you must make the users aware that the information will be available to your Product, and **you must provide legally adequate privacy notice and protection for those users.** Further, your Product may only use that information for the limited purposes for which the user has given you permission to do so. If your Product stores personal or sensitive information provided by users, it must do so securely and only for as long as it is needed. . . .

4.4 **Prohibited Actions.** You agree that **you will not engage in any activity** with the Market, including the development or distribution of Products, that interferes with, disrupts, damages, or **accesses in an unauthorized manner the devices, servers, networks, or other properties or services of any third party including, but not limited to, Android users,** Google or any mobile network operator. You

may not use customer information obtained from the Market to sell or distribute Products outside of the Market.

92. In order to publish and distribute an App over the Android Market, Google also requires App developers to execute and comply with its Android Software Development Kit License Agreement (a true and correct copy of which is available at <http://developer.android.com/sdk/terms.html>). Google's Android Software Development Kit License Agreement contains similar provisions mimicking the language in the two preceding paragraphs.

#### **Amazon.com's Android Appstore**

93. Amazon.com also owns and operates its own online digital distribution system and service for the sale and distribution of Apps compatible with wireless mobile devices running Google's Android operating system, which it calls the "Amazon.com: Appstore for Android."<sup>29</sup> Amazon.com opened the Appstore for Android in March of 2011. In a January 31, 2012 press release, Amazon.com announced that:

"Amazon Appstore for Android customers nearly tripled in the fourth quarter [of 2011] compared to the third quarter. In addition, customers downloaded more apps from the Amazon Appstore during the fourth quarter than they had during all previous quarters combined."

94. Amazon.com also maintains a rigorous approval and validation process for Apps published and distributed over its Appstore for Android and places restrictions on the types of Apps that can be published, sold or distributed over its

---

<sup>29</sup> See Amazon.com: Appstore for Android at <http://www.amazon.com/mobile-apps/b?ie=UTF8&node=2350149011>



Appstore for Android. In agreements with App developers, Amazon.com maintains the right to remove Apps from its Appstore for Android. Amazon.com has also issued at <https://developer.amazon.com/help/faq.html#> the following Appstore Developer Program Approval Process and Content Guidelines (as excerpted and emphasized below):

## Approval Process and Content Guidelines

### How does the app approval process work?

Our goal is for customers to have a good experience with every app they buy from the Amazon Appstore. As a result, **we will be testing the apps** you submit prior to making them available in our store **to verify that each app** works as outlined in your product description, **does not** impair the functionality of the mobile device or **put customer data at risk** once installed, and complies with the terms of the Appstore Distribution Agreement and our Content Guidelines. . . .

When you submit an app in the Developer Portal, the Amazon Appstore team will start the app review process. . . . If we have a question about your app during the review process or determine it does not meet one of the Amazon Appstore's acceptance criteria, we will notify you using the email address associated with your account and provide guidance on next steps. . . .

### Do my apps need to comply with a content policy?

Each app that you submit to us must adhere to the following Content Guidelines. If we determine that an app contains, facilitates, or promotes content that is prohibited by these guidelines, we will reject the app submission and notify you using the email address associated with your developer account.

### Content Guidelines

Please take a moment to familiarize yourself with a few examples of prohibited content:

- **Offensive Content:** What we deem offensive is probably about what you would expect. We reserve the right to determine the appropriateness of all apps and to accept or reject any app at our discretion. We also have full discretion to publish maturity ratings for the apps.
- **Pornography:** We prohibit apps containing pornography or hard-core material that depict graphic sexual acts or sexually explicit

material. We also don't allow content that drives traffic to pornography sites.

- **Illegal Activity:** Each app must comply with all applicable laws. We prohibit apps that promote or may lead to the production of an illegal item or illegal activity. Developers are responsible for researching to ensure that each app is in compliance with all local, state, national, and international laws.
- **Intellectual Property Infringement:** We prohibit any app to which you do not have the necessary rights to make available in the Amazon Appstore or that violates our Copyright Policy (see below).
- **Privacy/Publicity Infringement:** ***We hold personal privacy in the highest regard. Therefore, we prohibit apps that infringe, or have the potential to infringe, upon an individual's privacy, right of publicity, or that portray an individual in a false light.*** Celebrity images and/or celebrity names cannot be used for commercial purposes without permission of the celebrity or their management. This includes unauthorized celebrity image collections.
- **Copyright Policy:** Amazon's Appstore Distribution Agreement requires that you have ownership or license rights to the code and content (including advertising) included in any app. Do not upload any app if you do not have the rights listed in the Appstore Distribution Agreement. You are responsible for ensuring that you hold necessary rights to distribute the app through the Amazon Appstore. If you are unsure if you own all rights to the app, please consult an attorney.

. . . We will also notify you by email when the status of your app changes. You will receive an email when:

- Your app successfully completes our testing process and is published in the Amazon Appstore. . . .
- Your app has failed our testing process. We will provide you with details on the failure and will also provide guidance on resubmission.

95. Amazon.com charges developers a \$99 annual fee to participate in the Appstore Developer Program and to be eligible to distribute and sell Apps over its Appstore for Android.<sup>30</sup>

---

<sup>30</sup> See Amazon's App Approval Process and Content Guidelines at <https://developer.amazon.com/help/faq.html#Approval Process and Content Guidelines>.

96. Consequently, via their mobile App marketplace storefronts, Apple, Google and Amazon.com each act as facilitators, gatekeepers and digital distribution partners for the distribution and sale of third-party Apps compatible with iOS- and Android-based wireless mobile devices and each of them contractually and in practice maintain significant control over content and availability of each App that is eventually released and made available to the public over their respective App marketplaces.

**PLAINTIFFS MAINTAINED PRIVATE ADDRESS BOOK DATA ON  
THEIR IOS- AND ANDROID-BASED WIRELESS MOBILE DEVICES  
AND USED THE DEVICES AS PDAS, AS INTENDED BY THE DEVICES' DESIGNERS**

97. Each Plaintiff named in this lawsuit owns one of the following wireless mobile devices: a smartphone operating on Apple's iOS platform (i.e., an Apple iPhone), an Android smartphone operating on Google's Android platform, or a wireless enabled iOS tablet or hand-held computer (e.g., an iPad or an iPod Touch). Each of these wireless mobile devices is capable of and was designed to run Apps.

98. Each Plaintiff has transferred to and maintains personal address book data, including contact names, phone numbers, physical and e-mail addresses, job titles, birthdays and other similarly private information (hereafter collectively, "Address Book Data"), on his or her wireless mobile device.

99. Because both iOS- and Android-based wireless mobile devices come pre-installed with Apps and software for "syncing" and storing the owner's Address Book Data as well as calendar, scheduling and alarm/reminder Apps, both types of devices

are designed, in part, to function and be used by their owners as mobile personal digital assistants (“PDAs”).

100. When connected to a designated computer network or laptop or desktop computer by the device’s owner, pre-installed software on both iOS- and Android-based wireless mobile devices automatically sync the wireless mobile device (via wire, wirelessly or over a network) to the designated computer system and automatically or on demand communicates and transfers to and stores on the wireless mobile device the owner’s private Address Book Data (oftentimes along with other calendaring and scheduling information and, if selected, music, video and photo files and Apps). This process is commonly known as “syncing” the wireless mobile device.

101. Each Plaintiff in this action has used and uses his or her respective iOS- or Android- based wireless mobile device, in part, in one of its intended manners as a personal digital assistant. Accordingly, each Plaintiff’s wireless mobile device contains a vast array of Plaintiff’s personal information, data, collections of data and files—including Address Book Data—all of which constitute personal property owned by each Plaintiff.<sup>31</sup>

102. Plaintiffs and all Class members have a reasonable expectation of privacy in the personal information, data, collections of data and files that they have input to,

---

<sup>31</sup> See Apple’s *Address Book Programming Guide for iOS* at p. 25 (wherein Apple admits that “**the Address Book database is ultimately owned by the user**”) (emphasis added) (attached as Exhibit 1).

transferred onto and maintain on their iOS- or Android- based wireless mobile devices—including and especially their Address Book Data.

103. Each Plaintiff in this action has transferred his or her private Address Book Data from another computer to his or her respective wireless mobile device via a syncing process. This syncing process constitutes an “electronic communication” within the meaning of the federal and state statutes identified this Complaint.

104. Each Plaintiff in this action has also manually input a small percent of his or her Address Book Data directly into his or her respective wireless mobile device (via, for example, the device’s keyboard).

105. The syncing and input of such Address Book Data results in the fixation of that data and information in a medium on each Plaintiff’s wireless mobile device.

106. Each Plaintiff’s private Address Book Data contained on his or her wireless mobile device is the personal property of the respective Plaintiff.

107. Each previously-identified wireless mobile device owned by each Plaintiff constitutes both a “computer” and a “protected computer” within the meaning of the federal and state statutes identified this Complaint.

**THE APPLICATION DEVELOPER DEFENDANTS—WITH APPLE’S AND OTHERS’ ASSISTANCE AND APPROVAL—CREATED AND DISTRIBUTED TROJAN-HORSE APPS THAT HACK WIRELESS MOBILE DEVICES AND STEAL THE OWNERS’ PRIVATE ADDRESS BOOK DATA**

108. Chart I, displayed below, lists several Apps that the identified Defendants created, produced, approved, marketed and/or distributed and identifies the respective

company developer, platform availability, initial availability date (where known), and sales or use volume to date (where known) of each App:

**Chart I. Application Developer Defendants' App Platform Availability.**

		<b>Platforms Offering the App and Date of First Availability (where known)</b>			
<b>App Product Name</b>	<b>Defendant App Developer</b>	<b>Apple's AppStore</b>	<b>Google's Android Market</b>	<b>Amazon.com's Appstore for Android</b>	<b>Number of Users</b>
<b>Path</b>	<i>Path</i>	Nov. 2010	Available		> 2,000,000
<b>Twitter</b>	<i>Twitter</i>	Available	Available	Available	
<b>Facebook</b>	<i>Facebook</i>	Available	Available	Available	> 300,000,000
<b>Instagram*</b>	<i>Instagram/ Burbn</i>	Oct. 2010	--	--	> 4,500,000
<b>Foursquare</b>	<i>Foursquare</i>	Mar. 2009	Available	Available	> 15,000,000
<b>Gowalla**</b>	<i>Gowalla</i>	2007	Available	Available	> 600,000
<b>Beluga***</b>	<i>Beluga</i>	Until 2011	Until 2011		
<b>Foodspotting</b>	<i>Foodspotting</i>	Available	Available	Available	> 1,000,000
<b>Yelp!</b>	<i>Yelp!</i>	Available	Available	Available	> 4,500,000
<b>Hipster</b>	<i>Hipster</i>	Available	Available		
<b>LinkedIn</b>	<i>LinkedIn</i>	Available	Available	Available	
<b>Angry Birds</b>	<i>Rovio</i>	Available	Available	Available	
<b>Cut the Rope***</b>	<i>ZeptoLab</i>	Available	Available	Available	> 60,000,000
<b>Kik Messenger</b>	<i>Kik Interactive</i>	Available	Available		> 8,000,000

\* On information and belief, Instagram acquired the Instagram App from Burbn and is its successor-in-interest.

\*\* On information and belief, Facebook acquired the Gowalla App and Gowalla's staff in December 2011 and is its successor-in-interest. The 600,000 user figure is as of November 2010.

\*\*\* On information and belief, Facebook acquired the BelugaApp and Beluga's staff in December 2011 and is its successor-in-interest.

\*\*\*\* On information and belief, ZeptoLab's Cut the Rope App is published and distributed through Chillingo, which became a division of Electronic Arts on October 19, 2011.

109. Defendants Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and

ZeptoLab are hereafter collectively referred to as the “Application Developer Defendants.”

110. On information and belief, Apple has tested and approved each of the Apps identified in Chart I for distribution to iPhone, iPad and iPod Touch wireless mobile devices over its AppStore. Apple has posted and distributes to iPhone, iPad and iPod Touch wireless mobile devices each of the Apps identified in Chart I via Apple’s AppStore.

111. On information and belief, except for the Instagram App, Google has tested and approved each of the Apps identified in Chart I for distribution to Android-based wireless mobile devices over its Android Market.

112. On information and belief, except for the Instagram App, Amazon.com has tested and approved each of the Apps identified in Chart I for distribution to Android-based wireless mobile devices over its Appstore for Android.

113. On information and belief, each of the Application Developer Defendants listed in Chart I has entered into agreements with Apple, Google and/or Amazon.com to abide by their respective App content policies, including policies prohibiting distribution of Apps that access, copy, upload, or use any wireless mobile device owner’s private data or information without explicit authorization. On information and belief, each Application Developer Defendant distributing an App over the AppStore was informed in writing prior to release of its App that the address book databases

contained on wireless mobile devices are owned by the user of the wireless mobile device.

114. However, in contravention of those agreements and without the permission or effective consent of the wireless mobile device's owner, on information and belief, each Application Developer Defendant by means of its App identified in Chart I nevertheless accesses, copies, uploads, transfers and/or uses in interstate commerce the device owner's private Address Book Data from the wireless mobile device. The Application Developer Defendants' actions in this regard constitute knowingly accessing a computer, computer network, computer system or data and copying, transferring and using such data without the express effective consent of the owner; interception or use of electronic communications; and theft, misappropriation and conversion of personal property within the meaning of the federal and state statutes identified in this Complaint.

115. Each App identified in Chart I is installed on at least one named Plaintiff's or Class member's wireless mobile device and, for each identified mobile operating system, was procured from at least one defendant's digital distribution platform. Chart II identifies each respective App and the digital distribution platform (*i.e.*, App storefront) from which it was procured by each Plaintiff:



**Chart II. Plaintiffs' Apps and Procurement Sources.**

	<b>Storefront from which Plaintiffs acquired Apps</b>	
<b><u>App</u></b>	<b><u>Apple's AppStore</u></b>	<b><u>Google's Android Market</u></b>
<b>Path</b>	Judy Long, Marc Opperman, Jason Green	
<b>Twitter</b>	Marc Opperman, Claire Moses, Gentry Hoffman, Steve Dean, Alan Beurshasen, Greg Varner, Rachelle King, Giuli Biondi, Nirali Mandaywala, Jason Green	Alicia Medlock, Scott Medlock
<b>Facebook</b>	Marc Opperman, Claire Moses, Steve Dean, Alan Berchausen, Rachelle King, Giuli Biondi, Nirali Mandaywala, Jason Green	Alicia Medlock, Scott Medlock
<b>Instagram</b>	Marc Opperman, Gentry Hoffman, Greg Varner, Jason Green, Rachelle King, Giuli Biondi, Jason Green	
<b>Foursquare</b>	Gentry Hoffman, Alan Beurshasen, Greg Varner, Nirali Mandaywala	
<b>Gowalla</b>	Steve Dean, Alan Beurshasen, Greg Varner, Rachelle King, Nirali Mandaywala	
<b>Beluga</b>	[Facebook has recently shuttered the Beluga service]	
<b>FoodSpotting</b>	Rachelle King	
<b>Yelp!</b>	Claire Moses, Gentry Hoffman, Giuli Biondi, Nirali Mandaywala	
<b>Hipster</b>	Rachelle King	
<b>LinkedIn</b>	Marc Opperman, Steve Dean, Giuli Biondi	Alicia Medlock, Scott Medlock
<b>Kik Messenger</b>	Jason Green	
<b>Angry Birds</b>	Marc Opperman, Claire Moses, Steve Dean, Beurshasen, Greg Varner, Nirali Mandaywala, Jason Green	
<b>Cut the Rope</b>	Claire Moses, Greg Varner, Giuli Biondi, Nirali Mandaywala, Jason Green	

116. Plaintiffs have not given the Application Developer Defendants effective consent to access, upload, transfer and/or use their Address Book Data contained on their wireless mobile devices.

117. On information and belief, the Application Developer Defendants have nevertheless accessed, uploaded, transferred and/or used in interstate commerce for their own purposes at least a portion of the Plaintiffs' and the Class members' private Address Book Data maintained on their wireless mobile devices.

118. The Application Developer Defendants' actions relating to the Plaintiffs' private Address Book Data was inherently undiscoverable by the Plaintiffs and was not discovered by Plaintiffs until sometime after the publication of an article on February 8, 2012 describing how Defendant Path's Path App accessed used such address book data without prior permissions. Accordingly, to the extent necessary, Plaintiffs assert the discovery rule and the doctrine of equitable tolling with respect to each of their claims in this action.

119. On information and belief, the Application Developer Defendants' actions were facilitated and assisted by the digital distribution platform owners—particularly Apple—who provided the Application Developer Defendants with tutorials, pre-written code and instructions for designing Apps that would both access and upload users' private Address Book Data from their wireless mobile devices and who turned a blind eye to violations of their own respective App content policies, agreements and

testing and verification procedures when they allowed each of the Application Developer Defendants' Apps identified in Chart I to be distributed to the market over their respective App digital delivery platforms.

120. Unfortunately, these oversights do not appear to be an aberration. In fact, according to a published NEW YORK TIMES reports,

*The address book in smartphones — where some of the user's most personal data is carried — is free for app developers to take at will, often without the phone owner's knowledge. . . . Companies that make many of the most popular smartphone apps for Apple and Android devices — Twitter, Foursquare and Instagram among them — routinely gather the information in personal address books on the phone and in some cases store it on their own computers.*

\* \* \*

*While Apple says it prohibits and rejects any app that collects or transmits users' personal data without their permission, that has not stopped some of the most popular applications for the iPhone, iPad and iPod — like Yelp, Gowalla, Hipster and Foodspotting — from taking users' contacts and transmitting it without their knowledge.<sup>32</sup>*

On information and belief, the NEW YORK TIMES article quoted immediately above accurately describes conduct engaged in by each of the respective defendants in this action who are discussed in the article.

121. On information and belief, Apple has the ability to remotely disable Apps, even after they have been distributed and installed on wireless mobile devices.

122. Notably, the United States Federal Trade Commission has urged the White House to increase Internet privacy measures, especially for mobile devices and

---

<sup>32</sup> See Nicole Peroth and Nick Bilton, *Mobile Apps Take Data Without Permission*, NEW YORK TIMES (online ed. at [www.nytimes.com](http://www.nytimes.com) and <http://bits.blogs.nytimes.com/2012/02/15/google-and-mobile-apps-take-data-books-without-permission/> Feb. 15, 2012) (emphasis added).

social networks, stating that federal laws have not kept up with the Apps to ensure that personal information isn't being improperly used.<sup>33</sup>

123. In late February 2012, California's attorney general lamented in a press release that **"Your personal privacy should not be the cost of using mobile apps, but all too often it is."**

124. Moreover Google, Apple, Amazon.com and several other large technology companies entered into a recent agreement with California's attorney general regarding App privacy policies and protecting App users' privacy.

125. On March 5, 2012, "United States Senator Charles E. Schumer [also] called for the Federal Trade Commission to launch an investigation into reports that smartphone applications sold on the Apple and Android platforms are allowed to steal private photos and customers address books."<sup>34</sup>

126. On information and belief, in mid-February 2012, Apple stated to press outlets in response to privacy concerns raised regarding App address book data harvesting issues that Apps which surreptitiously harvest and upload a user's address book data without the user's prior consent violate Apple's developer agreements.

127. Specifically, Apple spokesman Tom Neumayr said:

---

<sup>33</sup> See Kang, Cecilia, *FTC, White House urge Internet privacy measures*, THE WASHINGTON POST (Mar. 16, 2011) at [http://www.washingtonpost.com/blogs/post-tech/post/ftc-white-house-urge-internet-privacy-measures/2011/03/16/AB8AQoe\\_blog.html](http://www.washingtonpost.com/blogs/post-tech/post/ftc-white-house-urge-internet-privacy-measures/2011/03/16/AB8AQoe_blog.html).

<sup>34</sup> See Press Release dated March 5, 2011, U.S. SENATOR CHARLES E. SCHUMER'S OFFICIAL WEBSITE at <http://schumer.senate.gov/Newsroom/record.cfm?id=336191>.

“Apps that collect or transmit a user's contact data without their prior permission are in violation of our guidelines.”<sup>35</sup>

Nevertheless, with respect to any of the Defendants’ offending Apps complained of herein, Apple has not removed any of the Apps from Apple’s AppStore, disabled any of the Apps or terminated or suspended any of the Defendants’ AppStore accounts.<sup>36</sup>

### **Path admits wrongdoing when caught uploading Users’ Address Book Data**

128. Path operates a social networking-enabled photo sharing and messaging service for mobile devices. According to Path’s website, Path’s synonymously-named Path App is a “smart journal that helps you share life with the ones you love.”<sup>37</sup> As of early February 2012, Path had over two million users.<sup>38</sup>

129. Path was formed in late 2010. Path has received over \$11 million in funding in its short year-and-a-half existence. Path received an initial \$2.5 million

---

<sup>35</sup> Lowenson, Josh, *Apple: Apps using address data are in violation, fix to come*, C|NET ONLINE (Feb. 15, 2012) at [http://news.cnet.com/8301-27076\\_3-57378551-248/apple-apps-using-address-data-are-in-violation-fix-to-come/#ixzz1oTQ22Tw9](http://news.cnet.com/8301-27076_3-57378551-248/apple-apps-using-address-data-are-in-violation-fix-to-come/#ixzz1oTQ22Tw9).

<sup>36</sup> On information and belief, Apple similarly and, on information and belief, knowingly allowed the Unknown App Developers’ contractually non-compliant Apps having stealth address-book-data-harvesting functionalities—which each similarly wrongfully access owners’ wireless mobile devices and harvest the device owner’s Address Book Data without the owner’s prior effective consent—to pass through Apple’s supposedly stringent testing and approval procedures discussed above and to be marketed, sold and distributed over Apple’s AppStore to consumers, including the Plaintiffs and the Class members..

<sup>37</sup> See Path’s About Us website at <https://path.com/about>.

<sup>38</sup> See Path’s About Us website at <https://path.com/about>.

funding from Index Ventures, First Round Capital and Ashton Kutcher, among others,<sup>39</sup> and a second round in February 2011 of \$8.5 million from venture capital firms Kleiner Perkins Caufield & Byers, Index Ventures and Digital Garage of Japan<sup>40</sup> at a reported \$25 million valuation.<sup>41</sup> Path has less than 50 employees.

130. According to published reports and on information and belief, Google previously made an offer of roughly \$100,000,000 to acquire Path, which equates to approximately \$5 per Path user or \$4 million per present Path employee.<sup>42</sup>

131. Path launched and released its Path App around November, 2010. Path distributes its Path App through the specified digital distribution platforms identified in Chart I. The specified Plaintiffs identified in Chart II obtained the Path App from the designated App storefront(s) and have installed and used the Path App on their respective wireless mobile device(s).

132. In early February, 2011, news reports and web blogs reported that for several months Path's App had been automatically and surreptitiously accessing, harvesting and uploading to Path's computer servers—for Path's own undisclosed use—complete copies of the users' "contact data" (i.e., the Address Book Data described

---

<sup>39</sup> Isaac, Mike, *New Social Network Path = iPhone + Instagram + Facebook – 499,999,950 Friends*, FORBES (November 14, 2010) at <http://blogs.forbes.com/mikeisaac/2010/11/14/new-social-network-path-iphone-instagram-facebook-499999950-friends/>.

<sup>40</sup> See <http://gigaom.com/2011/02/01/path-gets-8-5-million-ahem-why/>.

<sup>41</sup> See [http://articles.businessinsider.com/2011-02-02/tech/29977989\\_1\\_facebook-employees-arrington-path](http://articles.businessinsider.com/2011-02-02/tech/29977989_1_facebook-employees-arrington-path)

<sup>42</sup> See *id.*

above) maintained on a Path user's wireless mobile device without first obtaining the wireless mobile device owner's consent.

133. Notably, prior to that revelation, Path had conversely stated on one of its websites touting its Path App that "Path upholds the expectations for privacy of both the mobile phone and the journal with its limited, intimate, more personal network."<sup>43</sup>

134. Similarly, Path's CEO had previously stated in 2010 in a responsive e-mail to a technology reporter that "Path does not retain or store any of [the user's] information in any way." This statement was false.<sup>44</sup>

135. Not surprisingly, many Path users have publicly expressed outrage over Path's previously undisclosed accessing, storage and use of the private Address Book Data maintained on their wireless mobile devices. On information and belief, in the week following these news reports, Path experienced a decline in Path App installations, a drop in drop in traffic over Path's network, and increased incidents of cancellation of Path accounts.

136. On information and belief, Path has, in fact, knowingly and intentionally accessed, used, uploaded, stored and/or transferred to Path and/or other third parties at least a portion of the private Address Book Data previously transferred onto and

---

<sup>43</sup> See Path's "Story website at <https://path.com/story> .

<sup>44</sup> See Tate, Ryan, *Don't Forgive Path, the Creepy iPhone Company that Misled Us Once Already*, GAWKER at <http://gawker.com/5883549> and Rafe Needleman, *Path's Dave Morin: No, really I don't lie about this stuff*, C|NET ONLINE (Feb. 8, 2012) [http://news.cnet.com/8301-19882\\_3-57373704-250/paths-dave-morin-no-really-i-dont-lie-about-this-stuff/](http://news.cnet.com/8301-19882_3-57373704-250/paths-dave-morin-no-really-i-dont-lie-about-this-stuff/).

maintained on its App users' (including Plaintiffs' and the class members') wireless mobile device(s) running the Path App without the users' (including Plaintiffs' and the Class members') prior effective consent. On information and belief, Path re-accesses and/or retransmits this private Address Book Data at regular and/or irregular intervals (possibly as frequently as once per day).

137. After being caught red-handed stealing its users' Address Book Data and in response to the accompanying firestorm of negative publicity, on February 8, 2012, Path's founder and CEO, Doug Morin, offered the following apology on Path's company website (a true and correctly copy of which is copied in full below):





Blog

About

Story

Questions

Team

Jobs

Path 2.0.6

## We are sorry.

We made a mistake. Over the last couple of days users brought to light an issue concerning how we handle your personal information on Path, specifically the transmission and storage of your phone contacts.

As our mission is to build the world's first personal network, a trusted place for you to journal and share life with close friends and family, we take the storage and transmission of your personal information very, very seriously.

Through the feedback we've received from all of you, we now understand that the way we had designed our 'Add Friends' feature was wrong. We are deeply sorry if you were uncomfortable with how our application used your phone contacts.

In the interest of complete transparency we want to clarify that the use of this information is limited to improving the quality of friend suggestions when you use the 'Add Friends' feature and to notify you when one of your contacts joins Path—nothing else. We always transmit this and any other information you share on Path to our servers over an encrypted connection. It is also stored securely on our servers using industry standard firewall technology.

We believe you should have control when it comes to sharing your personal information. We also believe that actions speak louder than words. So, as a clear signal of our commitment to your privacy, we've deleted the entire collection of user uploaded contact information from our servers. Your trust matters to us and we want you to feel completely in control of your information on Path.

In Path 2.0.6, released to the App Store today, you are prompted to opt in or out of sharing your phone's contacts with our servers in order to find your friends and family on Path. If you accept and later decide you would like to revoke this access, please send an email to [service@path.com](mailto:service@path.com) and we will promptly see to it that your contact information is removed.

We care deeply about your privacy and about creating a trusted place for you to share life with your close friends and family. As we continue to expand and grow we will make some mistakes along the way. We commit to you that we will continue to be transparent and always serve you, our users, first.

We hope this update clears up any confusion. You can find Path 2.0.6 in the App Store [here](#).

Sincerely,



Dave Morin  
Co-Founder and CEO

457

Feb 8 2012

138. On information and belief, Mr. Morin is an officer, director and agent of Path and is authorized to speak on Path's behalf. Mr. Morin's attached blog post on behalf of Path as cited in the preceding paragraph constitutes an admission by a party opponent in this action. Mr. Morin's attached blog post is admissible in this action to prove liability on the part of Path on the claims asserted by Plaintiffs and the Class members herein.

139. Moreover, Mr. Morin's attached blog post also constitutes an admission by Path of Path's (and its agents') intentional destruction of and/or tampering with evidence of a crime—which is an additional felony. *E.g.*, TEX. PENAL CODE § 37.09 (c) and (d)(1); *see also* 18 U.S.C. 1512(c)(1) (obstruction of justice by evidence tampering). On information and belief, Mr. Morin and Path were advised and/or instructed by others to follow this course of action.

140. Path's deletion from its servers and/or records of such illegally obtained data also constitutes destruction and spoliation of evidence.

141. In the annotated and highlighted excerpt of Mr. Morin's statement (excerpted immediately below), Path admits to knowingly and intentionally accessing, scanning, copying, transmitting, using and storing at least a portion of its users' private Address Book Data that users had transferred to and maintained on their wireless mobile devices:

***We made a mistake.*** Over the last couple of days users brought to light an issue concerning how **we handle your personal information** on Path, specifically **the**

**transmission and storage of your phone contacts.** . . [W]e take the storage and transmission of your personal information very, very seriously. . . [and] we now understand that **the way we had designed our 'Add Friends' feature was wrong.** . . **[O]ur application used your phone contacts.** . . . the use of this information is limited **to improving** the quality of [Path's] friend suggestions [service] . . . **and to notify you when one of your contacts joins Path . . . We [] transmit this . . . information . . . to our servers . . . It is also stored [ ] on our servers.** . . We believe you should have control when it comes to sharing your personal information. . . . . , **we've deleted the entire collection of user uploaded contact information** from our servers. . . . In Path 2.0.6, released to the App Store today, **you are [now] prompted to opt in or out of sharing your phone's contacts with our servers . . .** We care deeply about your privacy . . .

142. On information and belief, Path has been accessing, copying, harvesting, using and/or storing its users' wireless mobile device's Address Book Data since at early as November 2010 (*i.e.*, for approximately 450 days as of the filing of this lawsuit).

143. On information and belief, Path's App repeatedly harvests, transfers and remotely stores its users' wireless mobile device Address Book Data on a regular basis and at regular intervals.

144. On information and belief, Path's regular frequency for conducting these operations is as frequent as once per day.

145. Path's hollow, public-relations driven apology and supposed subsequent deletion of its users' illegally stolen private Address Book Data (even if true) does not rectify Path's prior 15 months of illegal data harvesting, usage and storage operations (no matter what the supposed purpose of those operations may have been) or the damages flowing from those acts. Nor does it prevent Path users from being harmed similarly in the future.

146. Plaintiffs and the Class members have been harmed by Path's wrongful conduct and have suffered actual damages.

147. On information and belief, Path's wrongful access and use of the Plaintiffs' and the Class members' private Address Book Data has also allowed Path to establish and facilitate additional network data points and networked connections among users within its social networking business operations, which has allowed Path to increase its advertising rates and revenues and has enhanced Path's corporate valuation for fundraising and other purposes.

148. Path has been unjustly enriched by its actions described herein.

149. On information and belief, Path's wrongful conduct described herein will continue unless enjoined by this Court.

150. Plaintiffs and the Class members have no adequate remedy at law.

**Like Path, the other Application Developer Defendants engage in similar *illegal conduct* with respect to their App User's wireless mobile devices' private Address Book Data<sup>45</sup>**

151. As result of recent revelations regarding Path, myriad technical blogs and news reports have posted assessments of various Apps and issued lists and descriptions of Apps that (according to such reports and posts) without the owners' or users' prior

---

<sup>45</sup> Throughout the remainder of this Complaint, collective allegations regarding the Application Developer Defendants' conduct and the harm suffered by the Plaintiffs and the Class members are intended to be interpreted as those actions and resulting harms attributable to the specific Application Developer Defendants whose Apps are on Plaintiffs' (and the Class members') respective wireless mobile devices, as identified in Chart II above. On information and belief, with Apple's knowledge, similar conduct was engaged in and harmed caused by the Unknown App Developers and their Apps.

permission or effective consent also appear to access, scan, copy, transmit, upload, use and/or store partial or full copies of the App user's mobile wireless device's private Address Book Data that users had previously transferred to and maintain on their wireless mobile devices.<sup>46</sup>

152. On information and belief, the other Application Developer Defendants named in this suit—and additional App development companies (known at this time to Apple but not to Plaintiffs) whose Apps have similar Trojan-horse functionalities but are nevertheless distributed over the AppStore (i.e., the Unknown Application Developers)—have engaged in similar *illegal conduct* and actions with respect to their App users' wireless mobile device's private Address Book Data.

153. Unlike Path, though, the majority of other Application Developer Defendants have not, as of yet, specifically acknowledged, apologized for or attempted to rectify the harm inflicted by those wrongful actions and similar *illegal conduct*.

154. On information and belief and as further described below, without the owners' prior permission or effective consent, each of the other Application Developer Defendants (and the other Unknown Application Developers) have knowingly and intentionally accessed, scanned, copied, transmitted, uploaded, used and/or stored partial or full copies of their App users'—including the Plaintiffs' and Class members'—wireless mobile device's private Address Book Data that users previously transferred to

---

<sup>46</sup> See, e.g., Nicole Peroth and Nick Bilton, *Mobile Apps Take Data Without Permission*, NEW YORK TIMES (online ed. at [www.nytimes.com](http://www.nytimes.com), Feb. 15, 2012).

and maintained on their wireless mobile devices, via their respective Twitter, Facebook, Instagram, Foursquare, Gowalla, Beluga, FoodSpotting, Yelp!, Hipster, LinkedIn, Kik Messenger, Angry Birds, Cut a Rope and other as-of-yet unidentified Apps.

155. On information and belief, each Application Developer Defendant (and each Unknown App Developer) engaged and in this wrongful and illegal activity and will continue to engage in such wrongful, harmful and illegal conduct unless enjoined by this Court.

156. Apple, Google and Amazon.com continue to make each of the previously identified Apps—all of which expressly violate Apple, Google and Amazon.coms' own App developer policies and agreements and, as discussed herein, enable and facilitate the commission of federal and state crimes including wiretapping, fraud in relation to and breach of computer security, interception of, access to, copying of and/or use of electronic communications and computer data as well as garden variety theft, misappropriation and conversion of iPhone, iPad, iPod Touch and Android device owners' property and invasion of their privacy—available to the public on their respective AppStore, Android Market and Appstore for Android digital distribution platforms at further risk of additional serious harm to the public and continue to support each of the Apps on their respective iOS- and Android- mobile operating systems.

157. Put another way, though Apple, Google and Amazon.com either are or reasonably should have known via their respective testing and approval procedures that the Application Developer Defendants (and the other Unknown App Developers) are eavesdropping on their customers and stealing customers' private Address Book Data via their Apps, not only have Apple, Google and Amazon.com done little to stop it, they actually facilitated those actions by approving, marketing, distributing and supporting those Apps knowing that they had such illegal and supposedly-prohibited functionalities.

158. The Plaintiffs' and the Class members' private Address Book Data (including the discrete identifying contact data points contained and aggregated therein) that the Defendants (and the Unknown App Developers) illegally harvested and wrongfully obtained has marketable commercial value in excess of a nominal sum. For example, according to one publication the market value of and per-contact going rate for the purchase of similar contact information currently ranges from a minimum of around \$0.60 *per contact* up to several dollars *per contact*.<sup>47</sup>

159. Consequently, the Defendants and the Unknown App Developers have been unjustly enriched by their actions describe herein.

---

<sup>47</sup> See PointFlex Cost Per Lead by Industry Report at <http://www.slideshare.net/sumitkroy/pontiflex-cost-per-lead-by-industry> (containing studies estimating prices from approximately \$0.60 to in excess of \$3.00 per discrete contact).

160. The Plaintiffs and the Class members have been harmed by the Defendants' (and the Unknown App Developers') conduct and wrongful activities and have suffered actual damages.

161. Plaintiffs and the Class members have no adequate remedy at law.

### **Twitter**

162. Twitter owns and operates an online social networking and micro-blogging service. Twitter's synonymously-named Twitter App enables its users to send and read text-based posts of up to 140 characters, commonly known as "tweets." As of 2011, Twitter's service had over 300 million users with in excess of 140 million tweets posted daily.

163. Twitter was formed in 2006. Twitter received an \$800 million investment in 2010 that at the time was reported to be the largest venture capital investment round in history; raised an additional \$200 million in venture capital in December 2010 at a valuation of approximately \$3.7 billion; and received an additional \$300 million investment in December 2011 from the Saudi prince Alwaleed bin Talal at an \$8.4 billion company valuation.

164. Twitter distributes its Twitter App through the specified digital distribution platforms identified in Chart I. The specified Plaintiffs identified in Chart II obtained the Twitter App from the designated App storefront(s) and have installed and used the Twitter App on their respective wireless mobile device(s).



165. Recent published reports, such as the above-referenced NEW YORK TIMES article, indicate that the Twitter App “routinely” accesses, uses, uploads, stores and/or transfers the App user’s private Address Book Data maintained on his or her wireless mobile device running the Twitter App without first obtaining the device owner’s consent. On information and belief, the Twitter App accesses, copies, uses, uploads and/or transfers at least a portion of the private Address Book Data contained in a wireless mobile device running the Twitter App without first obtaining the mobile device owner’s prior effective consent.

166. Twitter has acknowledged that its App scans and uploads its App users’ complete set Address Book Data. Twitter has also admitted that it regularly stores the e-mail addresses and phone numbers obtained from its App users’ Address Book Data sets on Twitter’s own computer systems for up to 18 months.

167. Prior to February 7, 2012, Twitter had not informed its App users that it would be storing portions of their Address Book Data for any period of time.

168. On information and belief, Twitter has knowingly and intentionally accessed, copied used, uploaded, stored and/or transferred to Twitter and/or other third parties at least a portion of the private Address Book Data previously transferred to and maintained on Plaintiffs’ wireless mobile device(s) running the Twitter App without Plaintiffs’ prior effective consent. On information and belief, Twitter re-accesses and/or

retransmits this private Address Book Data at regular and/or irregular intervals (possibly as frequently as once per day).

169. Plaintiffs and the Class members have been harmed by Twitter's wrongful conduct and have suffered actual damages.

170. On information and belief, Twitter's wrongful access and use of the Plaintiffs' and the Class members' private Address Book Data has also allowed Twitter to establish and facilitate additional network data points and networked connections among users within its social networking business operations, which has allowed Twitter to increase its advertising rates and revenues and has enhanced Twitter's corporate valuation for fundraising and other purposes.

171. Twitter has been unjustly enriched by its actions described herein.

172. On information and belief, Twitter's wrongful conduct described herein will continue unless enjoined by this Court.

173. Plaintiffs and the Class members have no adequate remedy at law.

### **Facebook**

174. Facebook is the world's largest social networking service and is now used by approximately 845 million people. Facebook's synonymously-named Facebook App is available on both iOS- and Android-based mobile devices. More than 425 million active users access Facebook through mobile devices across 200 mobile operators in 60

countries. Nearly 45% of the people who use Facebook access it through the Facebook mobile App.

175. Facebook was formed in 2004. In 2011, Facebook announced \$3.7 billion in annual revenues and \$1 billion in profits. Advertising accounted for approximately 85% of Facebook's 2011 revenues. Facebook is presently scheduled to go public in one of, if not the, largest initial public stock offerings in history. Facebook's anticipated post-IPO valuation is \$75 billion to \$100 billion, which will make its CEO and founder Mark Zuckerberg's personal net worth somewhere around \$24 billion.<sup>48</sup>

176. Facebook has been dogged by privacy concerns regarding its acquisition, harvesting and use of its users' data. Around November 29, 2011, Facebook agreed to settle U.S. Federal Trade Commission charges that it deceived consumers by failing to keep privacy promises.

177. Facebook distributes its Facebook App through the specified digital distribution platforms identified in Chart I. The specified Plaintiffs identified in Chart II obtained the Facebook App from the designated App storefront(s) and have installed and used the Facebook App on their respective wireless mobile device(s).

178. Recent published reports indicate that the Facebook App accesses, copies, uses, uploads, stores and/or transfers the private Address Book Data contained in a user's wireless mobile device running the Facebook App without first obtaining the

---

<sup>48</sup> See USA TODAY (online ed. Feb. 1, 2012) at <http://www.usatoday.com/tech/news/story/2012-02-01/facebook-ipo/52921528/1>.

device owner's consent. On information and belief, the Facebook App accesses, copies, uses, uploads, stores and/or transfers at least a portion of the private Address Book Data maintained on a user's wireless mobile device running the Facebook App without first obtaining the device owner's effective consent.

179. On information and belief, Facebook has knowingly and intentionally accessed, copied, used, uploaded and/or transferred to Facebook and/or other third parties at least a portion of the private Address Book Data previously transferred to and contained in Plaintiffs' wireless mobile device(s) running the Facebook App without Plaintiffs' prior effective consent. On information and belief, Facebook re-accesses and re-transmits this private Address Book Data at regular and/or irregular intervals (possibly as frequently as once per day).

180. Plaintiffs and the Class members have been harmed by Facebook's wrongful conduct and have suffered actual damages.

181. On information and belief, Facebook's wrongful access and use of the Plaintiffs' and the class members' private Address Book Data has also allowed Facebook to establish and facilitate additional network data points and networked connections among users within its social networking business operations, which has allowed Facebook to increase its advertising rates and revenues and has enhanced Facebook's corporate valuation.

182. Facebook has been unjustly enriched by its actions described herein.

183. On information and belief, Facebook's wrongful conduct described herein will continue unless enjoined by this Court.

184. Plaintiffs and the Class members have no adequate remedy at law.

### **Yelp!**

185. Yelp! owns and operates a social networking, user review and local search service. Yelp!'s synonymously-named Yelp! App enables its users to read, write and post such reviews and search for local establishments from their wireless mobile devices. Yelp!'s service currently has 60 million unique monthly visitors across 13 countries.

186. Yelp! was formed in 2004. Yelp! had an initial public offering of its stock on March 2, 2012, which was priced to raise approximately \$100 million at a company valuation of \$778 million.<sup>49</sup>

187. In November 2011, Yelp! acknowledged a user data privacy breach affecting iPhone and Android smartphone users,<sup>50</sup> which was revealed when a team of

---

<sup>49</sup> See Barbara Ortutay, *Yelp soars 64% on first day of trading after IPO*, USA TODAY (online ed., Mar. 2, 2012) at <http://www.usatoday.com/money/industries/technology/story/2012-03-02/yelp-ipo-first-day/53331544/1>; *Yelp Another Overvalued IPO from Bubble 2.0*, SEEKING ALPHA, at <http://seekingalpha.com/article/377211-yelp-another-overvalued-ipo-from-bubble-2-0>,

<sup>50</sup> See Yelp! Online blog at <http://engineeringblog.yelp.com/2011/10/output-filtering-failure.html> (Yelp! engineering response to data disclosure issue).

professors “identified a large-scale privacy vulnerability at Yelp.com that was leaking private records of Yelp subscribers to users of their mobile site.”<sup>51</sup>

188. Yelp! distributes its Yelp! App through the specified digital distribution platforms identified in Chart I. The specified Plaintiffs identified in Chart II obtained the Yelp! App from the designated App storefront(s) and have installed and used the Yelp! App on their respective wireless mobile device(s).

189. Recent published reports indicate that the Yelp! App accesses, copies, uses, uploads, stores and/or transfers at least a portion of the private Address Book Data maintained on a wireless mobile device running the Yelp! App without first obtaining the device owner’s consent. On information and belief, the Yelp! App accesses, copies, uses, uploads, stores and/or transfers at least a portion of the private Address Book Data maintained on a user’s wireless mobile device running the Yelp! App without first obtaining the device owner’s effective consent.

190. On information and belief, Yelp! has knowingly and intentionally accessed, copied, used, uploaded, stored and/or transferred to Yelp! and/or other third parties at least a portion of the private Address Book Data previously transferred to and maintained in Plaintiffs’ wireless mobile device(s) running the Yelp! App without Plaintiffs’ prior effective consent. On information and belief, Yelp! re-accesses and

---

<sup>51</sup> See <http://www.bu.edu/hic/2011/11/02/yelp-privacy-breach/>.

retransmits this private Address Book Data at regular and/or irregular intervals (possibly as frequently as once per day).

191. Plaintiffs and the Class members have been harmed by Yelp!'s wrongful conduct and have suffered actual damages.

192. On information and belief, Yelp!'s wrongful access and use of the Plaintiffs' and the class members' private Address Book Data has also allowed Yelp! to establish and facilitate additional network data points and networked connections among users within its social networking business operations, which has allowed Yelp! to increase its advertising rates and revenues and has enhanced Yelp!'s corporate valuation.

193. Yelp! has been unjustly enriched by its actions described herein.

194. On information and belief, Yelp!'s wrongful conduct described herein will continue unless enjoined by this Court.

195. Plaintiffs and the Class members have no adequate remedy at law.

### **Instagram**

196. Instagram's synonymously-named Instagram App is a photo sharing application that allows users to take a photo, apply a digital filter, then share it with a variety of social networking services including Instagram's own. Instagram has over 10 million users and over 150 million user photos have been uploaded through Instagram's service.

197. Instagram was formed in 2010. In February 2011, Instagram raised \$7 million in a series A venture capital funding round. On information and belief, Burbn is a predecessor-in-interest of Instagram, at least with respect to the Instagram App, and Instagram and Burbn are affiliated in some way.

198. The Instagram App launched on Apple's App Store on approximately October 6, 2010. Apple named the Instagram App as its "App of the Year" for 2011. Presently, Instagram is only available on the iPhone and iPad.

199. Prior to February 2012, the Instagram App did not comply with the privacy or user-data policies specified in either Apple's App developer policies cited above or the written developer agreements between Apple and Instagram. Apple was aware of this non-compliance. Apparently, an App's non-compliance with Apple's own App Store policies and developer agreements is not a disqualifier for Apple's "App of the Year" award.

200. Instagram distributes its Instagram App through the specified digital distribution platforms identified in Chart I. The specified Plaintiffs identified in Chart II obtained the Instagram App from the designated App storefront(s) and have installed and used the Instagram App on their respective wireless mobile device(s).

201. Recent published reports indicate that the Instagram App accesses, uses, copies, uploads, stores and/or transfers the private Address Book Data maintained on a wireless mobile device running the Instagram App without first obtaining the device



owner's consent. On information and belief, the Instagram App accesses, uses, copies, uploads, stores and/or transfers at least a portion of the private Address Book Data maintained on a user's wireless mobile device running the Instagram App without first obtaining the device owner's effective consent.

202. On information and belief, Instagram has knowingly and intentionally accessed, copied, used, uploaded and/or transferred to Instagram and/or other third parties at least a portion of the private Address Book Data previously transferred to and maintained on Plaintiffs' wireless mobile device(s) running the Instagram App without Plaintiffs' prior effective consent. On information and belief, Instagram re-accesses and/or retransmits this private address book data at regular and/or irregular intervals.

203. Plaintiffs and the Class members have been harmed by Instagram's wrongful conduct and have suffered actual damages.

204. On information and belief, Instagram's wrongful access and use of the Plaintiffs' and the Class members' private Address Book Data has also allowed Instagram to establish and facilitate additional network data points and networked connections among users within its social networking business operations, which has allowed Instagram to increase its advertising rates and/or revenues and has enhanced Instagram's corporate valuation for fundraising and other purposes.

205. Instagram has been unjustly enriched by its actions described herein.

206. On information and belief, Instagram's wrongful conduct described herein will continue unless enjoined by this Court.

207. Plaintiffs and the Class members have no adequate remedy at law.

### **Foursquare Labs**

208. Foursquare Labs owns and operates a location-based social networking service for mobile devices such as smartphones. Foursquare Lab's Foursquare App enables its users to "check in" at and receive points, coupons or awards from various locations. (The App also makes recommendations to users—essentially targeted ads—of future locations where users might wish to "check in.") Foursquare Labs reported that it had 10 million registered users as of June 2011 and now averages over 3 million "check ins" per day.

209. Foursquare Labs was formed in 2009. In June 2011, Foursquare Labs received a \$50 million investment that valued the company at approximately \$600 million.

210. Foursquare Labs distributes its Foursquare App through the specified digital distribution platforms identified in Chart I. The specified Plaintiffs identified in Chart II obtained the Foursquare App from the designated App storefront(s) and have installed and used the Foursquare App on their respective wireless mobile device(s).

211. Recent published reports indicate that the Foursquare App accesses, copies, uses, uploads, stores and/or transfers the private Address Book Data maintained

on a wireless mobile device running the Foursquare App without first obtaining the device owner's consent. According to a February 15, 2012 reports in the NEW YORK TIMES entitled *Mobile Apps Take Data Without Permission* and on information and belief, prior to that date when users signed up for a Foursquare account via an iPhone, iPad, iPod or Android phone, Foursquare transmitted the device's address book information to Foursquare Labs without prior warning. On information and belief, the Foursquare App accesses, copies, uses, uploads, stores and/or transfers at least a portion of the private Address Book Data maintained on a user's wireless mobile device running the Foursquare App without first obtaining the device owner's effective consent.

212. On information and belief, Foursquare Labs has knowingly and intentionally accessed, used, uploaded and/or transferred to Foursquare Labs and/or other third parties at least a portion of the private Address Book Data previously transferred to and contained in Plaintiffs' wireless mobile device(s) running the Foursquare App without Plaintiffs' prior effective consent. On information and belief, Foursquare Labs re-accesses and/or retransmits this private Address Book Data at regular and/or irregular intervals.

213. Erin Gleason is (or was at the time of the following quote) Foursquare Labs' director of communications. Ms. Gleason has stated in written e-mails to press personnel that, "When a person searches for friends on Foursquare, *we transmit the address book information* over a secure connection and do not store it beyond that

point.” On information and belief, the portion of Ms. Gleason’s previously quoted statement concerning transmission of address book information is an accurate quote, is true, constitutes an admission of a party opponent and is admissible against Foursquare Labs in this action.

214. Plaintiffs and the Class members have been harmed by Foursquare Lab’s wrongful conduct and have suffered actual damages.

215. On information and belief, Foursquare Lab’s wrongful access and use of the Plaintiffs’ and the class members’ private Address Book Data has also allowed Foursquare Labs to establish and facilitate additional network data points and networked connections among users within its social networking business operations, which has allowed Foursquare Labs to increase its advertising rates and revenues and has enhanced Foursquare Lab’s corporate valuation for fundraising and other purposes.

216. Foursquare Labs has been unjustly enriched by its actions described herein.

217. On information and belief, Foursquare Labs’s wrongful conduct described herein will continue unless enjoined by this Court.

218. Plaintiffs and the Class members have no adequate remedy at law.

## Gowalla

219. Gowalla is a location-based social network. Gowalla's synonymously-named Gowalla App allows users to "check in" at spots in their local vicinity and receive virtual awards. As of January 2011, Gowalla's service had over 600,000 users.

220. Gowalla was formed in 2007. Gowalla raised \$8.4 million in capital in 2009. In December 2011, Gowalla (and/or its assets and employees) were acquired by Facebook for an undisclosed sum. According to a blog post written by Gowalla's founders," Gowalla is Going to Facebook."<sup>52</sup> On information and belief, Facebook is a successor-in-interest to Gowalla's obligations and liabilities.

221. Gowalla distributes its Gowalla App through the specified digital distribution platforms identified in Chart I. The specified Plaintiffs identified in Chart II obtained the Gowalla App from the designated App storefront(s) and have installed and used the Gowalla App on their respective wireless mobile device(s).

222. Recent published reports indicate that the Gowalla App accessed, copied, used, uploaded, stored and/or transferred the private Address Book Data maintained on a wireless mobile device running the Gowalla App without first obtaining the device owner's consent. On information and belief, the Gowalla App accessed, copied, used, uploaded, stored and/or transferred at least a portion of the private Address Book Data

---

<sup>52</sup> See Gowalla blog at <http://blog.gowalla.com/post/13782997303/gowalla-going-to-facebook> .

maintained on a user's wireless mobile device running the Gowalla App without first obtaining the device owner's effective consent.

223. On information and belief, Gowalla has knowingly and intentionally accessed, copied, used, uploaded and/or transferred to Gowalla and/or other third parties at least a portion of the private Address Book Data previously transferred to and maintained on Plaintiffs' wireless mobile device(s) running the Gowalla App without Plaintiffs' prior effective consent. On information and belief, Gowalla re-accesses and/or retransmits this private Address Book Data at regular and/or irregular intervals (possibly as frequently as once per day).

224. Plaintiffs and the Class members have been harmed by Gowalla's wrongful conduct and have suffered actual damages.

225. On information and belief, Gowalla's wrongful access and use of the Plaintiffs' and the Class members' private Address Book Data also allowed Gowalla to establish and facilitate additional network data points and networked connections among users within its social networking business operations, which allowed Gowalla to increase its advertising rates and revenues and enhanced Gowalla's desirability and valuation for acquisition purposes.

226. Gowalla (and its successor-in-interest) have been unjustly enriched by their actions described herein.

227. On information and belief, Gowalla's (and/or its successor-in-interest's) wrongful conduct described herein will continue unless enjoined by this Court.

228. Plaintiffs and the Class members have no adequate remedy at law.

### **Beluga**

229. Beluga is a group mobile messaging service. Beluga's synonymously-named Beluga App allowed users to instantly message groups of wireless mobile device users.

230. Beluga was formed and launch in mid-2010. Around early March 2011, Beluga (and/or its assets, technology and employees) were acquired by Facebook for an undisclosed sum. On information and belief, Facebook is a successor-in-interest to Beluga's obligations and liabilities and has incorporated Beluga's technology into its own services. Facebook recently shuttered the pre-existing Beluga service.

231. Beluga distributed its Beluga App through the specified digital distribution platforms identified in Chart I. The specified Plaintiffs identified in Chart II obtained the Beluga App from the designated App storefront(s) and have installed and used the Beluga App on their respective wireless mobile device(s).

232. Recent published reports indicate that the Beluga App accessed, copied, used, uploaded, stored and/or transferred the private Address Book Data maintained on a wireless mobile device running the Beluga App without first obtaining the device owner's consent. On information and belief, the Beluga App accessed, copied, used,

uploaded, stored and/or transferred at least a portion of the private Address Book Data maintained on a user's wireless mobile device running the Beluga App without first obtaining the device owner's effective consent.

233. On information and belief, Beluga has knowingly and intentionally accessed, copied, used, uploaded and/or transferred to Beluga and/or other third parties (including, on information and belief, to Facebook) at least a portion of the private Address Book Data previously transferred to and maintained on Plaintiffs' wireless mobile device(s) running the Beluga App without Plaintiffs' prior effective consent. On information and belief, Beluga re-accessed, retransmitted and/or used this private Address Book Data at regular and/or irregular intervals (possibly as frequently as once per day).

234. Plaintiffs and the Class members have been harmed by Beluga's wrongful conduct and have suffered actual damages.

235. On information and belief, Beluga's wrongful access and use of the Plaintiffs' and the Class members' private Address Book Data also allowed Beluga to establish and facilitate additional network data points and networked connections among users within its social networking business operations, which allowed Beluga to increase its advertising rates and revenues and enhanced Beluga's desirability and valuation for acquisition purposes.



236. Beluga (and its successor-in-interest) have been unjustly enriched by their actions described herein.

237. On information and belief, Beluga's (and/or its successor-in-interest's) wrongful conduct described herein will continue unless enjoined by this Court.

238. Plaintiffs and the Class members have no adequate remedy at law.

### **Foodspotting**

239. Foodspotting owns and operates a food-related social networking service. Foodspotting's synonymously-named FoodSpotting App allows its users to find and share food recommendations and photos. Foodspotting now has over two million users.

240. Foodspotting was formed in 2010 and has raised \$3.75 million dollars in venture capital to date.

241. Foodspotting distributes its FoodSpotting App through the specified digital distribution platforms identified in Chart I. The specified Plaintiffs identified in Chart II obtained the FoodSpotting App from the designated App storefront(s) and have installed and used the FoodSpotting App on their respective wireless mobile device(s).

242. Recent published reports indicated that the FoodSpotting App accesses, copies, uses, uploads, stores and/or transfers the private Address Book Data maintained on a wireless mobile device running the FoodSpotting App without first clearly

obtaining the device owner's consent. On information and belief, the FoodSpotting App accesses, copies, uses, uploads, stores and/or transfers at least a portion of the private Address Book Data maintained on a wireless mobile device running the FoodSpotting App without first clearly obtaining the device owner's effective consent.

243. On information and belief, Foodspotting has knowingly and intentionally accessed, copied, used, uploaded and/or transferred to Foodspotting and/or other third parties at least a portion of the private Address Book Data previously transferred to and maintained on Plaintiffs' wireless mobile device(s) running the FoodSpotting App without Plaintiffs' prior effective consent. On information and belief, Foodspotting re-accesses, retransmits and/or uses this private address book data at regular and/or irregular intervals.

244. Until February, 2012, if a FoodSpotting wireless mobile device user pressed the "Find iPhone Contacts" button in the FoodSpotting App running on an iPhone, the App would access the user's iPhone's *entire* address book and, without the user's prior explicit consent, then (i) upload at least the e-mail address portions of the user's Address Book Data stored on the iPhone to Foodspotting's computer servers, (ii) on information and belief then cross-reference the user's surreptitiously uploaded Address Book Data against Foodspotting's own internal database of information, and (iii) use the user's surreptitiously uploaded Address Book Data to create additional data points and interlinked nodes on Foodspotting's own internal database of networked

user contacts. A true and correct copy of a Foodspotting corporate blog post from Foodspotting's <http://www.foodspotting.com/blog?category=News> website—in which Foodspotting acknowledges that it engaged in these alleged acts—is copied below:

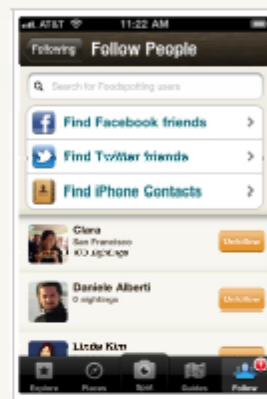
## News

### Finding iPhone Contacts on Foodspotting: How it works & how we're improving it

Update on 2/19: You can now [download Foodspotting 3.2](#) for iPhone which addresses the security concern below & adds an additional confirmation after you tap Find iPhone Contacts.

You may or may not have been hearing about recent [concerns](#) spreading throughout the [tech press](#) regarding how iPhone apps are using your address book con.ac.s.

*We wanted to reassure you that Foodspotting never has and never will use your iPhone contacts without your permission. The only time address book info is ever sent to Foodspotting is when you explicitly ask us to find friends from your address book by tapping, "Follow People > Find iPhone Contacts," and we never store any of this data on our servers.*



That said, in light of recent concerns, we're taking extra precautions to make this process even more transparent and secure in the future.

#### When does Foodspotting access my address book contacts?

As a convenience for users, we offer a "Find iPhone Contacts" feature. The only time your con.ac.s are ever sent to Foodspotting is when you use this feature. We use your friends' email addresses to check if any of your friends are on Foodspotting, show you the results and delete your address book data. No phone numbers or names are transferred.

#### What are the concerns?

Mos. of the concerns have been around apps that upload and store iPhone Contacts without users knowing. We've never done that, but it additionally turns out that while your address book data is being sent to Foodspotting using version 3.1 or earlier (which only takes seconds), there is a very slight chance that hackers could access your con.ac.s' email addresses if they happen to be on the same Wi-Fi network as you and monitoring your activity. (When doing any online activities on an unsecure Wi-Fi network, you're subject to this sort of risk.) It only applies to Foodspotting users' iPhone Contacts when and if you are logged in and use "Find iPhone Contacts" before our next update.

#### How is Foodspotting addressing these concerns?

In light of these concerns, we've added additional levels of security Foodspotting 3.2. We'll also be requesting an additional permission after you tap "Find iPhone Contacts."

#### What if I don't want to send my contacts to Foodspotting?

Simply avoid using "Find iPhone Contacts." You can always find friends using Facebook or Twitter, which you can securely connect to Foodspotting.



Posted by [Ted Grubbin News](#)  
on February 15, 2012



1



1

2

245. On information and belief, the person who posted the blog cited in the preceding paragraph is an officer, director and/or authorized agent of Foodspotting and was authorized to post the blog statement on Foodspotting's behalf. Foodspotting's blog post constitutes an admission by a party opponent in this action and is admissible in this action to prove liability on the part of Foodspotting on the claims asserted by Plaintiffs and the Class members herein.

246. Foodspotting has conclusively admitted for the purposes of this lawsuit via the previously-cited Foodspotting blog post that Foodspotting has knowingly and intentionally accessed, copied, transmitted and used at least portions of its users' Address Book Data that users' had previously transferred to and maintained on their wireless mobile devices.

247. On information and belief, Foodspotting continues to use and has not deleted or uncoupled the networked contact data points created in its computer file system database via the use of its users' surreptitiously uploaded Address Book Data and information.

248. Plaintiffs and the Class members have been harmed by Foodspotting's wrongful conduct and have suffered actual damages.

249. On information and belief, Foodspotting's wrongful access and use of the Plaintiffs' and the Class members' private Address Book Data has also allowed Foodspotting to establish and facilitate additional network data points and networked

connections among users within its social networking business operations, which has allowed Foodspotting to increase its advertising rates and revenues and has enhanced Foodspotting's corporate valuation for fundraising and other purposes.

250. Foodspotting has been unjustly enriched by its actions described herein.

251. On information and belief, Foodspotting's wrongful conduct described herein will continue unless enjoined by this Court.

252. Plaintiffs and the Class members have no adequate remedy at law.

### **Hipster**

253. Hipster owns and operates a social networking location-based photo sharing service. According to Hipster's website, Hipster's synonymously-named Hipster App allows users to "share where you are and what you're doing with postcards of your photos."

254. Hipster was founded in 2010 and is backed in part by Google Ventures, the venture capital arm of Google, Inc.

255. Hipster distributes its Hipster App through the specified digital distribution platforms identified in Chart I. The specified Plaintiffs identified in Chart II obtained the Hipster App from the designated App storefront(s) and have installed and used the Hipster App on their respective wireless mobile device(s).

256. Recent published reports, including the previously cited NEW YORK TIMES report, indicate that the Hipster App accesses, copies, uses, uploads, stores and/or

transfers the private Address Book Data maintained on a wireless mobile device running the Hipster App without first obtaining the mobile device owner's consent.<sup>53</sup> On information and belief, the Hipster App accesses, copies, uses, uploads, stores and/or transfers at least a portion of the private Address Book Data maintained on a user's wireless mobile device running the Hipster App without first obtaining the device owner's consent.

257. On information and belief, Hipster has knowingly and intentionally accessed, copied, used, uploaded, stored and/or transferred to Hipster and/or other third parties at least a portion of the private Address Book Data previously transferred to and maintained on Plaintiffs' wireless mobile device(s) running the Hipster App without Plaintiffs' prior effective consent. On information and belief, Hipster re-accesses, retransmits and uses this private Address Book Data at regular and/or irregular intervals.

258. Hipster admitted to uploading and using the e-mail addresses contained in its App users' wireless mobile devices' address book without asking the user for permission to do so.

259. On February 8, 2012, Hipster CEO Doug Ludow wrote the following guest post (copied in full below) on the TechCrunch website

---

<sup>53</sup> See also Pallab De, *Path, Hipster, and Several Other Mobile Apps Caught Uploading Contact List without Permission*, TECHIEBUZZ.COM (Feb. 8, 2012) at <http://techie-buzz.com/mobile-news/path-hipster-mobile-contact-list-privacy.html> .

<http://techcrunch.com/2012/02/08/hipster-ceo-also-apologizes-for-address-book-gate-calls-for-application-privacy-summit-guest-post/> acknowledging and apologizing for the Hipster App uploading its users' Address Book Data, admitting that **“we [Hipster] clearly dropped the ball when it comes to protecting our users' privacy,”** and calling on the leaders and CEOs of the mobile App industry to attend an “Application Privacy Summit” and adopt a “privacy pledge” to “help give their users sense of mind regarding their personal data.”:



# Hipster CEO Also Apologizes For Address Book-Gate, Calls For “Application Privacy Summit” [Guest Post]

DOUG LUDLOW

Wednesday, February 8th, 2012



*The following is a guest post from [Hipster](http://www.hipster.com) (<http://www.hipster.com>) CEO Doug Ludlow, (<http://www.cnn.com/2012/02/08/tech/hipster-ceo/index.html>) following yesterday and today's revelations that [select](http://www.techcrunch.com/2012/02/08/hipster-address-book/) (<http://www.techcrunch.com/2012/02/08/hipster-address-book/>) apps were uploading users' entire address books to their databases.*

We blew it, we're sorry, and we're going to make it right.

It's Hipster's goal to provide a fun and beautiful service for our community to share where they are, and what they are doing – creating a safe environment for our users is of the utmost importance to us. However, when we built our “Find Friends” feature for iOS, we clearly dropped the ball when it comes to protecting our users' privacy.

Yesterday, one of our Hipster users, Mark Chang (<http://markchang.tumblr.com/>) wrote a blog post detailing a few ways in which our “Find Friends” feature handles user privacy issues. You can read his post [here](http://markchang.tumblr.com/post/17244167951/hipster-uploads-part-of-your-iphone-address-book-to-its) (<http://markchang.tumblr.com/post/17244167951/hipster-uploads-part-of-your-iphone-address-book-to-its>).

Mark's criticisms were spot on, and needless to say we're pretty embarrassed by the situation. Embarrassed not because we had malicious goals in mind (we don't store the contact data we pull – we just match it to existing users), but embarrassed by the fact that we pushed a feature that doesn't meet our standards for the protection of our users' data.

How are we working to remedy the situation? In an update that will be available through iTunes this week, we've changed the way our “Find Friends” feature works on iOS. Rather than automatically pull in a user's contacts to help them find people already on Hipster, we're making this feature opt-in, and users will have to confirm that they want to grant access to their address book. In addition, this data will now be transferred through a SSL connection.

But where do we go from here?

We'd like to use our recent experience to help improve the mobile industry as a whole.

On Thursday, February 17<sup>th</sup>, we'll be hosting a “Application Privacy Summit” here at Hipster's SF office to discuss of user privacy in mobile applications.

In addition to discussing best practices and privacy standards, the goal of the summit is to come up with a “privacy pledge” – one that can be adopted by all apps, detailing for users what types of privacy expectations they should have. Applications will be able to boast that they have agreed to the privacy pledge, which should help give their users sense of mind regarding their personal data.

Invitations are being sent out to the CEOs of major mobile application companies, and we hope they will attend. In addition, if you're interested in attending, please email me at [Doug@Hipster.com](mailto:Doug@Hipster.com) (<mailto:Doug@Hipster.com>).

We made a mistake, but we hope that what we've learned will shed light on the need for clear standards when it comes to protecting user privacy. Doing so will only do great things for our industry, our companies, and most importantly, our users.

---

260. On information and belief, Mr. Ludow is an officer, director and agent of Hipster and is authorized to speak on Hipster's behalf. Mr. Ludow's guest post on behalf of Hipster as cited in the preceding paragraph constitutes an admission by a

party opponent in this action. Mr. Ludow's attached blog post is admissible in this action to prove liability on the part of Hipster on the claims asserted by Plaintiffs and the Class members herein.

261. Plaintiffs and the Class members have been harmed by Hipster's wrongful conduct and have suffered actual damages.

262. On information and belief, Hipster's wrongful access and use of the Plaintiffs' and the Class members' private Address Book Data has also allowed Hipster to establish and facilitate additional network data points and networked connections among users within its social networking business operations, which has allowed Hipster to increase its advertising rates and/or revenues and has enhanced Hipster's corporate valuation for fundraising and other purposes.

263. Hipster has been unjustly enriched by its actions described herein.

264. On information and belief, Hipster's wrongful conduct described herein will continue unless enjoined by this Court.

265. Plaintiffs and the Class members have no adequate remedy at law.

### **LinkedIn**

266. LinkedIn owns and operates a business-related social networking service. LinkedIn's synonymously-named LinkedIn App provides a mobile version of its online service. As of 2011, LinkedIn's service had over 150 million users.

267. LinkedIn was formed in 2003 and is now a public company with approximately \$250 million in annual revenues.

268. LinkedIn distributes its LinkedIn App through the specified digital distribution platforms identified in Chart I. The specified Plaintiffs identified in Chart II obtained the LinkedIn App from the designated App storefront(s) and have installed and used the LinkedIn App on their respective wireless mobile device(s).

269. Recent published reports indicate that the LinkedIn App accesses, copies, uses, uploads, stores and/or transfers the private address book data maintained on a wireless mobile device running the LinkedIn App without first obtaining the device owner's consent. On information and belief, the LinkedIn App accesses, copies, uses, uploads, stores and/or transfers at least a portion of the private Address Book Data maintained on a user's wireless mobile device running the LinkedIn App without first obtaining the device owner's effective consent.

270. On information and belief, LinkedIn has knowingly and intentionally accessed, copied, used, uploaded and/or transferred to LinkedIn and/or other third parties at least a portion of the private Address Book Data previously transferred to and maintained on Plaintiffs' wireless mobile device(s) running the LinkedIn App without Plaintiffs' prior effective consent. On information and belief, LinkedIn re-accesses, retransmits and/or uses this private Address Book Data at regular and/or irregular intervals.

271. Plaintiffs and the Class members have been harmed by LinkedIn's wrongful conduct and have suffered actual damages.

272. On information and belief, LinkedIn's wrongful access and use of the Plaintiffs' and the Class members' private Address Book Data has also allowed LinkedIn to establish and facilitate additional network data points and networked connections among users within its social networking business operations, which has allowed LinkedIn to increase its advertising rates and revenues and has enhanced LinkedIn's corporate valuation for fundraising and other purposes.

273. LinkedIn has been unjustly enriched by its actions describe herein.

274. On information and belief, LinkedIn's wrongful conduct described herein will continue unless enjoined by this Court.

275. Plaintiffs and the Class members have no adequate remedy at law.

#### **Kik Interactive**

276. Kik Interactive owns and operates a wireless mobile device messaging, texting and chat service. Kik Interactive's Kik Messenger App provides real time chat and messaging over the user's wireless mobile device. As of 2012, Kik Interactive had over 8 million users for its Kik Messenger App.

277. Kik Interactive was formed in 2009 and raised approximately \$8 million in venture capital in March 2011.

278. Kik Interactive distributes its Kik Messenger App through the specified digital distribution platforms identified in Chart I. The specified Plaintiffs identified in Chart II obtained the Kik Messenger App from the designated App storefront(s) and have installed and used the Kik Messenger App on their respective wireless mobile device(s).

279. Recent published reports indicate that the Kik Messenger App accesses, copies, uses, uploads, stores and/or transfers the private address book data maintained on a wireless mobile device running the Kik Messenger App without first obtaining the device owner's consent. On information and belief, the Kik Messenger App accesses, copies, uses, uploads, stores and/or transfers at least a portion of the private Address Book Data maintained on a user's wireless mobile device running the Kik Messenger App without first obtaining the device owner's effective consent.

280. In response to a blog inquiry on the Quora.com website <http://www.quora.com/Is-it-against-Apples-terms-to-automatically-without-permission-upload-your-iPhones-address-book> (a true and correct screenshot of which is copied below) concerning whether it was "against Apple's terms" for the Kik Messenger App "to automatically without permission upload your iPhone address book," Kik Interactive's CEO Ted Livingston responded with the following blog post on behalf of Kik Interactive:

[Sign up for free](#) to ask questions and discover great content.

[Kik Messenger](#) [Privacy](#) [iOS Development](#) [iPhone](#)

## Is it against Apple's terms to automatically without permission upload your iPhone's address book?

Kik Messenger is automatically uploading my address book to check my contacts against other users' contact details. Is this against any terms defined by Apple?

In practice, I can have people appear as "Suggested friends" only by having their email or phone number in my address book.

[Repost](#)


4 Answers

 **Ted Livingston, CEO of Kik**  
16 votes by Kevin Swan, Karamdeep Nijjar, Ashish Choudhary, (more)  
Ted Livingston from Kik (and new to Quora!)

As part of the Kik service, we suggest people you "may know" who are already on Kik. We do this by doing a one time scan of your address book to see if there is anyone already on Kik. Nothing is ever shared or stored (we need to update our privacy policy!)


Most of our users tell us they love this feature, but we have since been informed of a few rare use cases that could cause a bad experience. For this, we are extremely sorry. We are just testing a version of the clients that will allow users to opt out of this, which we will submit shortly. It's been a crazy 17 days...

[1 Comment](#) • [Repost](#) • 17:51 on Mon Nov 8 2010

 **Gustaf Alstromer, Making a Walkie Talkie @ Voxer**  
9 votes by Joseph Geiser, Kristin Kotlibadottir, Richard F. Burghause, (more)  
Yes it is. They are breaking the terms.  
• Kik Messenger does not give...  
(more)

[Sign up for free](#) to read the full text. [Login](#) if you already have an account.

[Comment](#) • [Repost](#) • 16:52 on Fri Nov 5 2010

 **Igal Perelman, Anything Mobile @ Voxer**  
1 vote by Gustaf Alstromer  
This is actually more serious, they do send messages to your contact... (more)

[Sign up for free](#) to read the full text. [Login](#) if you already have an account.

[2 Comments](#) • [Repost](#) • 18:08 on Fri Nov 5 2010

 **Jason Devitt, CEO of Mr. Number**  
They are clearly breaching Apple ToS, and it is serious. But all th... (more)

[Sign up for free](#) to read the full text. [Login](#) if you already have an account.

[1 Comment](#) • [Repost](#) • 17:39 on Fri Nov 5 2010

Add Answer

[Post to Board](#)

[Add Answer](#)

### Related Questions

Why doesn't Apple require users to click to accept before providing apps access to address book data?

Is Anon User correct in that Quora imports your Gmail address book without permission?

Path (company/product): Will Path regain trust as it deletes data uploaded from users' phone books without their permission?

Is it against Apple's terms to design an app that just opens up to Facebook mobile?

Path (company/product): Under what terms can law enforcement acquire the uploaded address books of Path users?

[See more related questions](#)

### Share Question

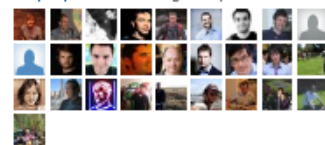
[Like](#) [Tweet](#) [6](#)

### Question Stats

Latest activity 17:51 on Mon Nov 8 2010.

This question has been viewed 1831 times; it has 2 monitors with 23767 topic followers and 0 aliases exist.

28 people are following this question.



281. On information and belief, Ted Livingston (i) is an officer, director and/or authorized agent of Kik Interactive, (ii) posted the blog post cited in the preceding paragraph, and (iii) was authorized to post the blog post cited in the preceding paragraph on Kik Interactive's behalf. Mr. Livingston's blog post cited in the preceding paragraph constitutes an admission by a party opponent in this action and is admissible in this action to prove liability on the part of Kik Interactive on the claims asserted by Plaintiffs and the Class members herein.

282. Kik Interactive has conclusively admitted for the purposes of this lawsuit via its CEO's cited blog post that Kik Interactive has knowingly and intentionally accessed and "scanned" its users' Address Book Data that users had previously transferred to and maintained on their wireless mobile devices.

283. On information and belief, Kik Interactive has knowingly and intentionally accessed, copied, used, uploaded and/or transferred to Kik Interactive and/or other third parties at least a portion of the private Address Book Data previously transferred to and maintained on Plaintiffs' wireless mobile device(s) running the Kik Messenger App without Plaintiffs' prior effective consent. On information and belief, Kik Interactive re-accesses, retransmits and/or uses this private Address Book Data at regular and/or irregular intervals.

284. Plaintiffs and the Class members have been harmed by Kik Interactive's wrongful conduct and have suffered actual damages.

285. On information and belief, Kik Interactive's wrongful access and use of the Plaintiffs' and the Class members' private Address Book Data has also allowed Kik Interactive to establish and facilitate additional network data points and networked connections among users within its social networking business operations, which has allowed Kik Interactive to increase its advertising rates and revenues and has enhanced Kik Interactive's corporate valuation for fundraising and other purposes.

286. Kik Interactive has been unjustly enriched by its actions describe herein.

287. On information and belief, Kik Interactive's wrongful conduct described herein will continue unless enjoined by this Court.

288. Plaintiffs and the Class members have no adequate remedy at law.

**Rovio (Angry Birds)**

289. Rovio makes, distributes and sells the Angry Birds gaming App, one of the most popular Apps of all time for wireless mobile devices. Over 12 million copies of the App have been purchased from Apple's App Store and, across all platforms (including wireless mobile devices, personal computers and gaming consoles) the game has been downloaded over 500 million times to date.

290. The Angry Birds App is a single-player video game where a user slingshots a series of birds at structures of the birds' enemy, the pigs, and scores points for toppling those structures.



291. Rovio distributes its Angry Birds App through the specified digital distribution platforms identified in Chart I. The specified Plaintiffs identified in Chart II obtained the Angry Birds App from the designated App storefront(s) and have installed and used the Angry Birds App on their respective wireless mobile device(s).

292. Recent published reports indicate that the Angry Birds App accesses, copies, uses, uploads, stores and/or transfers the private Address Book Data maintained on a wireless mobile device running the Angry Birds App without first obtaining the device owner's knowing consent.<sup>54</sup> On information and belief, the Angry Birds App accesses, uses, copies, uploads, stores and/or transfers the private Address Book Data maintained on a user's wireless mobile device running the Angry Birds App without first obtaining the device owner's knowing consent.

293. On information and belief, Rovio has knowingly and intentionally accessed, copied, used, uploaded and/or transferred to Rovio and/or other third parties at least a portion of the private Address Book Data previously transferred to and maintained on Plaintiffs' wireless mobile device(s) running the Angry Birds App without Plaintiffs' prior effective consent. On information and belief, Rovio re-accesses, retransmits and uses this private Address Book Data at regular and/or irregular intervals.

---

<sup>54</sup> See, e.g., *iOS consumers should Fear Angry Birds*, YOUR DAILY MAC at <http://www.yourdailymac.net/2011/04/ios-consumers-should-fear-angry-birds/>.

294. Plaintiffs and the Class members have been harmed by Rovio's wrongful conduct and have suffered actual damages.

295. On information and belief, Rovio has used and/or disclosed or sold to others at least portions the Plaintiffs' and the Class members' private Address Book Data.

296. Rovio has been unjustly enriched by its actions described herein.

297. On information and belief, Rovio's wrongful conduct described herein will continue unless enjoined by this Court.

298. Plaintiffs and the Class members have no adequate remedy at law.

**ZeptoLab, Chillingo & Electronic Arts (Cut the Rope App)**

299. ZeptoLab makes and Chillingo publishes, sells and distributes through the various digital download platforms the Cut the Rope gaming App. The Cut the Rope gaming App has been downloaded over 60 million times to date.

300. On information and belief, Chillingo was recently acquired by and now is a division of Electronic Arts. On information and belief, Electronic Arts is a successor-in-interest to Chillingo's obligations and liabilities. Consequently, on information and belief, ZeptoLab, Chillingo and Electronic Arts are jointly and severally liable on the claims alleged herein pertaining to the Cut a Rope App.

301. The Cut the Rope App is a single-player video game where a user makes slashing finger motions on the wireless mobile device screen to “cut” a “rope” so that fruit and other prizes fall into the mouth of a virtual monster.

302. The Cut the Rope App is distributed to users through the specified digital distribution platforms identified in Chart I. The specified Plaintiffs identified in Chart II obtained the Cut the Rope App from the designated App storefront(s) and have installed and used the Cut the Rope App on their respective wireless mobile device(s).

303. Recent published reports indicate that the Cut the Rope App accesses, copies, uses, uploads, stores and/or transfers the private Address Book Data maintained on a wireless mobile device running the Cut the Rope App without first obtaining the device owner’s consent. On information and belief, the Cut the Rope App accesses, copies, uses, uploads, stores and/or transfers at least a portion of the private Address Book Data maintained on a user’s wireless mobile device running the Cut the Rope App without first obtaining the device owner’s effective consent.

304. On information and belief, ZeptoLab has knowingly and intentionally accessed, copied, used, uploaded and/or transferred to ZeptoLab and/or other third parties at least a portion of the private Address Book data previously transferred to and maintained on Plaintiffs’ wireless mobile device(s) running the Cut the Rope App without Plaintiffs’ prior effective consent. On information and belief, ZeptoLab re-accesses, retransmits and uses this private Address Book Data at regular and/or

irregular intervals. On information and belief ZeptoLab has engaged in these actions with the assistance, support and/or encouragement of Chillingo and/or Electronic Arts.

305. Plaintiffs and the Class members have been harmed by ZeptoLab's, Chillingo's and Electronic Arts' wrongful conduct and have suffered actual damages.

306. On information and belief, ZeptoLab has used and/or disclosed or sold to others at least portions of the Plaintiffs' and the Class members' wrongfully accessed private Address Book Data.

307. On information and belief, Chillingo has knowingly and intentionally accessed, copied, used, uploaded, stored and/or transferred to Chillingo and/or other third parties at least a portion of the private Address Book Data previously transferred to and maintained on Plaintiffs' wireless mobile device(s) running the Cut the Rope App without Plaintiffs' prior effective consent. On information and belief, Chillingo re-accesses, retransmits and uses this private Address Book Data at regular and/or irregular intervals.

308. On information and belief, Chillingo has used and/or disclosed or sold to others at least portions of the Plaintiffs' and the Class members' private Address Book Data.

309. ZeptoLab, Chillingo and Electronic Arts have been unjustly enriched by their actions described herein.

310. On information and belief, ZeptoLab's, Chillingo's and Electronic Arts' wrongful conduct described herein will continue unless enjoined by this Court.

311. Plaintiffs and the Class members have no adequate remedy at law.

**UNDERLYING PREDICATE VIOLATIONS**<sup>55</sup>

312. Each Plaintiff, Class member and Defendant is a "person" within the meaning of all relevant statutes cited in this Complaint.

313. Each Plaintiff's and each Class member's respective wireless mobile device is a "computer" within the meaning of all relevant statutes cited in this Complaint.

314. Each Plaintiff's and each Class member's respective Address Book Data stored on his or her wireless mobile device constitutes "data" and "computer data" within the meaning of all relevant statutes cited in this Complaint.

315. Each Plaintiff's and each Class member's wireless mobile device and the compiled Address Book Data and discrete address book data stored on each such device is "property" within the meaning of all relevant statutes cited in this Complaint, including TEX. PENAL CODE § 33.01(16) (defining tangible property, intangible property and data as property) and TEX. PENAL CODE § 31.01(5).

---

<sup>55</sup> The allegations in this section apply equally to the actions of and the Apps of the Unknown App Developers.

316. Apple has admitted in Exhibit 1 that the Address Book Data contained on persons' iPhone, iPad and iPod Touch iOS wireless mobile devices is "owned" by the user of the device.

317. Each Application Developer Defendant's acts of communicating with its App user's wireless mobile device via its App or App-related service constitutes "accessing" such device within the meaning of all relevant statutes cited in this Complaint, including TEX. PENAL CODE §§ 16.02, 33.01(1) and CAL. PENAL CODE § 632, and each such communication is an "electronic communication" within the meaning of all relevant statutes cited in this Complaint.

318. Each Application Developer Defendant's respective App is an "electronic, mechanical or other device" within the meaning of all relevant statutes cited in this Complaint, including TEX. PENAL CODE § 16.02.

319. Each such alleged "access" by an Application Developer Defendant to any App user's wireless mobile device for either uploading or transferring to the Application Developer Defendant (and/or to other third parties) or subsequently using, analyzing, manipulating, or storing on the Application Developer Defendant's own computer systems at least a portion of the private Address Book Data from such device was intentional and knowing and was "unauthorized", "without authorization", "without permission" and "exceeded authorized access" or an "authorization for

access” within the meaning of all relevant statutes cited in this Complaint, including 18 U.S.C. § 1030(e)(1), TEX. PENAL CODE §§ 16.02 and 16.04, and CAL. PENAL CODE § 502.

320. Breach of Computer Security (TEX. PENAL CODE § 33.02(a)): Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab have each knowingly “accessed”<sup>56</sup> Plaintiffs’ and the Class members’ wireless mobile devices<sup>57</sup> —including by communicating with the device and accessing/retrieving portions or all of Plaintiffs’ compiled Address Book Data thereon—without Plaintiffs’ or the Class members’ effective consent, thereby committing a breach of computer security in violation of TEX. PENAL CODE § 33.02(a).

321. Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab each obtained a benefit from such actions constituting the breach and, in committing the actions constituting the breach, harmed Plaintiffs and the Class members. Based on the aggregated value of the data wrongfully accessed/retrieved from each App user and the aggregate mobile phone air time minutes consumed during such unauthorized retrievals, Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla,

---

<sup>56</sup> TEX. PENAL CODE § 33.01(1).

<sup>57</sup> The Plaintiffs’ and the Class members’ wireless mobile devices constitute “computers.” TEX. PENAL CODE § 33.01 (4). *See also* CAL. PENAL CODE § 502.

Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLabs' actions each constitute first degree felonies. See TEX. PENAL CODE § 33.02(b) and (c).

322. Application Developer Defendants' identified actions similarly constitute numerous violations of CAL. PENAL CODE § 502, which protects against the unauthorized access, copying or use of another's data or computer and provides, in part (emphasis added):

502. (a) It is the intent of the Legislature in enacting this section to expand the degree of *protection* afforded to individuals . . . *from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems*. . . . [T]he proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of *unauthorized access to computers, computer systems, and computer data*. . . . [P]rotection of the integrity of all types and forms of *lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals* as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data . . .

\* \* \*

(c) . . . [A]ny person who commits any of the following acts is *guilty of a public offense*:

(1) Knowingly accesses and without permission . . . uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) *Knowingly accesses and without permission [ ] copies, or makes use of any data from a computer, computer system, or computer network*, . . . whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

\* \* \*

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

\* \* \*



(d) (1) Any person who violates any of the provisions of [section 502(c) other than paragraph 9] . . . is punishable by a fine . . . or by imprisonment . . . for [up to three years] . . . or by both that fine and imprisonment . . .

\* \* \*

(e) (1) In addition to any other civil remedy available, *the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss* by reason of a violation of any of the provisions of subdivision (c) *may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. . . .*

(2) In any action brought pursuant to this subdivision *the court may award reasonable attorney's fees.*

\* \* \*

(4) In any action brought pursuant to this subdivision for a willful violation of the provisions of subdivision (c), where it is proved by clear and convincing evidence that a defendant has been guilty of oppression, fraud, or malice as defined in subdivision (c) of Section 3294 of the Civil Code, *the court may additionally award punitive or exemplary damages.*

(5) No action may be brought pursuant to this subdivision unless it is initiated within three years of the date of the act complained of, or the date of the discovery of the damage, whichever is later.

\* \* \*

(g) Any *computer, computer system, computer network, or any software or data, owned by the defendant, that is used during the commission of any public offense described in subdivision (c) or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of subdivision (c) shall be subject to forfeiture . . .*

323. Fraud and Related Activity in Connection with Computers (18 U.S.C. § 1030(a)(2)(C), (a)(4), and (a)(5) and (c)(4)(A)(i)(I) (w/aggregate 1-year loss greater than \$5,000) and (c)(4)(A)(i)(IV) (w/threat to public safety)): Each Plaintiff's (and each Class member's) wireless mobile device(s) are used in and affect interstate commerce; accordingly, the devices are "protected computers" within the meaning of 18 U.S.C. § 1030(a)(2)(C)) and TEX. PENAL CODE § 16.02. *See also* 18 U.S.C. § 1030(e)(1) and (e)(2)(B).

324. On information and belief, by their actions described herein, Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab have learned of, obtained and copied some or all of the wireless mobile device Address Book Data contents of Plaintiffs' and the Class members' who use their respective Apps beyond any prior authorization(s) expressly granted to them by Plaintiffs or the Class members. On information and belief, these actions were committed knowingly and intentionally by each of the identified defendants. Accordingly, the described actions of Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab all constitute violations of 18 U.S.C. § 1030(a)(2)(C).

325. On information and belief, the unauthorized processing, copying and/or uploading of Address Book Data intentionally initiated by Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab via their respective Apps on and from the Plaintiffs' and the Class members' wireless mobile devices resulted in the increased allocation and more rapid consumption of the wireless mobile device's processing power, memory resources, battery life and available cellular airtime minutes (which are paid for by the device owner), all of which constitute resulting damage and loss within

the meaning 18 U.S.C. § 1030(a)(5)(A) and (C)).<sup>58</sup> Accordingly, the described actions of Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab all constitute violations of 18 U.S.C. § 1030(a)(5)(A) and 18 U.S.C. § 1030(a)(5)(C).

326. On information and belief, each Application Developer Defendant's wrongful access to, copying, storing and uploading of its user's wireless mobile device's Address Book Data (hereafter, an "offense")—when aggregated across its multi-million user App install base—results in an aggregate loss in any one-year period well in excess of \$5,000 based upon (i) the estimated user-borne cost and/or market price for the purchase of the consumed cellular airtime for the aggregate yearly uploads, and (ii) the reasonable estimated aggregate annual cost for technical assistance and software for each victimized App user to validate the integrity of their wireless mobile device data and to respond to and plug the recently revealed security holes in their wireless mobile devices that have been exposed by each Application Developer Defendant's offenses. Accordingly, the described offenses of Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab each fall within 18 U.S.C. § 1030(c)(4)(A)(V).

---

<sup>58</sup> In Foodspotting's previous blog post copied above, Foodspotting has admitted that it takes "a few seconds" to upload each device's Address Book Data to its own servers. Alone, that figure may at first appear negligible; but aggregated across each Application Developer Defendant's many millions of users, that figure becomes very large, very quickly (particularly if the App frequently polls and reports back to the App developer's servers on any updated contents of a user's address book). For example, just one 3-second upload from each user of an App having a one-million user install-base amounts to the consumption in the aggregate of roughly 833 hours of wireless airtime.

327. On information and belief, each Application Developer Defendant's offenses—which, on information and belief, involve the scanning, copying and uploading of various data fields in its user-base's aggregate wireless mobile device Address Book Data over unsecured airwaves and unsecured wireless servers that the device might happen to connect to while running any of the complained-of Apps—causes a threat to public safety within the meaning of 18 U.S.C. § 1030(c)(4)(A)(IV) by, for example, exposing for electronic interception during transmission the contact information, addresses and similar private or even secret information for high level government employees and officials, first responders, military personnel, and government operatives—all of whom are quite likely to be members of or contacts of members of the Application Developer Defendants' App user-base or a user of the App themselves.

328. Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab each, as a result of their offenses, obtained something of value—*i.e.*, some or all of the data maintained on the Plaintiffs' (and the Class members') Address Book Data. On information and belief, each Application Developer Defendant had the requisite "intent to defraud" when it committed the offenses, as exemplified by each Application Developer Defendant's violations of the express terms, conditions and policies of their App development and distribution agreements with Apple, Google and Amazon.com,

which expressly and contractually prohibited the unauthorized copying, uploading, use and access of any App user's private data stored on their wireless mobile devices.

Accordingly, the described actions of Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab also constitute violations 18 U.S.C. § 1030(a)(4).

329. Wire Fraud (18 U.S.C. § 1343): Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab each obtained Plaintiffs' (and the Class members' wireless mobile devices' Address Book Data and information under false pretenses and as part of a scheme to defraud. The Application Developer Defendants caused their respective Apps, as well as the Plaintiffs' and the Class members' private Address Book Data, to both be transmitted as electronic signals in interstate commerce by means of wires and the airwaves for the purposes of and in furtherance of executing these schemes. Accordingly, the described actions of Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab constitute wire fraud under 18 U.S.C. § 1343.

330. On information and belief, Path, Twitter, Facebook, Yelp! , Instagram, Foursquare, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Messenger, Rovio and ZeptoLab have each divulged and/or disseminated the contents of Plaintiffs' and the Class members' private Address Book Data from Plaintiffs' and the Class members'

wireless mobile devices to, among others, (i) the Plaintiffs' and the Class members' wireless and/or cellphone service providers (*e.g.*, AT&T, Sprint or Verizon for iPhone users); (ii) any person or entity's server system that has an open wireless connection (say, a coffee shop or airport lounge) that the device happens to connect to while the App is uploading data and/or running either in the foreground or background on the device; (iii) Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab and their information technology personnel; and/or (iv) all persons who are data points in the wrongfully obtained Address Book Data who thereafter receive a contact notice, solicitation or connection via the Application Developer Defendant's respective App service.

331. Transportation of Stolen Property (18 U.S.C. § 2314 cl.2): As previously alleged, Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab each obtained Plaintiffs' and the Class members' property (*i.e.*, portions or all of their Address Book Data, which in the aggregate has a value well in excess of \$5,000) by means of false pretenses under a scheme to defraud. Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab have repeatedly transported that data and caused that data to be transported in interstate commerce (generally speaking, by sending it

over computer and wireless networks, including the World Wide Web) in furtherance of their schemes. Accordingly, the described actions of Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab constitute transportation of stolen property under 18 U.S.C. § 2314.

332. Theft of Property (TEX. PENAL CODE § 31.03): Wireless mobile devices are “property” under TEX. PENAL CODE § 31.01(5)(b). Personal address book data, whether in electronic or physical media—is also “property” under TEX. PENAL CODE § 31.01(5) (including both tangible and “intangible personal property,” such as data, within the definition of “property”). Plaintiffs and the Class members own their respective wireless mobile devices and their personal Address Book Data maintained and stored on those devices.

333. By their activities discussed herein, the Application Developer Defendants have “unlawful[ly]” “appropriated” each Plaintiff’s and each Class member’s wireless mobile device and at least a portion of the Address Book Data maintained on such wireless mobile device within the meaning of TEX. PENAL CODE §§ 31.01(4) and 31.03(b)(1). The uploading of each App user’s data from his or her wireless mobile device to the Application Developer Defendants’ computer systems constitutes a “transfer [of a] . . . non-possessory interest in the [user’s data] to” the Application Developer Defendants (and results in exposure of that data to any person or company

happening to have an intervening computer server in the data flow stream) and results in the consumption of airtime by the wireless mobile device while the Address Book Data is surreptitiously uploaded. Plaintiffs and the Class members did not “effectively consent” to either of these specified actions by the defendants.

334. Incident to the scanning and uploading of their Address Book Data, Plaintiffs and the Class members were deprived via the Application Developer Defendants’ Apps and systems of airtime on their wireless mobile devices as well as computing and processing power, resources and battery life. Moreover, Plaintiffs and the Class members were deprived of their data and/or the data’s value, in part because it is unlikely that any defendant will return or expunge from their computer systems and social networks the data, nodes and connections created therein based upon the App users’ appropriated Address Book Data.

335. Accordingly, Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab have committed theft under TEX. PENAL CODE § 31.03.<sup>59</sup> On information and belief, the value of all data stolen by each Application Developer Defendant is, in the aggregate, substantial and in excess of \$200,000. Accordingly, because each Application Developer Defendant’s thefts are part of one scheme, the

---

<sup>59</sup> See also CAL. PENAL CODE.



amounts may be aggregated under TEX. PENAL CODE § 31.09, resulting in first degree felonies under TEX. PENAL CODE § 31.03(e)(7).

336. Racketeering Influence & Corrupt Organizations (18 U.S.C. § 1962):

Violations of 18 U.S.C. §§ 1343 and 2314 are each predicate acts under the Racketeering Influence & Corrupt Organizations Act (18 U.S.C. § 1962, et seq.). *See* 18 U.S.C. §§ 1961(1). Each Application Developer Defendant is alleged above to have committed both of these predicate acts.

337. Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab (and each of the Unknown App Developers) each conducted or participated in the conduct of the affairs of an enterprise engaged in interstate commerce through a pattern of racketeering activity—here, numerous repeated instances of wire fraud and transportation of stolen property harmful to the Plaintiffs and the class member—in violation of 18 U.S.C. § 1962(c). Each of the Application Developer Defendants (and each of the Unknown App Developers) have formed and participate in enterprises or associations via each underlying Application Developer Defendant’s (and each Unknown App Developer’s) operation of social networks underlying each of their respective App services and, in conjunction with at least Apple via the AppStore’s (and via the Android Market’s) App-development, -verification, -approval, -distribution and -sales network and integrated advertising framework and the affiliation of and

between those companies that are and have been engaged in a pattern of racketeering activities. Additionally, the defendants have in combination and collaboration pursued the common purpose of making money illegally and contrary to their own announced policies and contractual obligations via the development, distribution, sale and promotion in interstate commerce of goods and services (i.e., the Application Developer Defendants' and the Unknown App Developers' distributed Apps) that when properly used by the public as intended and designed, not only facilitate but in most instances automatically and surreptitiously invade the user's privacy, trigger breaches of the user's computer security, and stealthily and automatically commit unauthorized disclosures and transmissions in interstate commerce of the users' private stored electronic communications (i.e., their Address Book Data) in violation of numerous federal and state criminal statutes. Put more succinctly, under Apple's oversight and control, Apple, the Application Developer Defendants and the Unknown App Developers are effectively making and distributing illegal electronic eavesdropping/wiretapping devices—*i.e.*, the offending Apps, particularly when combined with the wireless mobile device as intended by both Apple and App developers—that regularly surreptitiously capture and report back on App users' Address Book Data. This association exists separate and apart from the pattern of racketeering that is being pursued by these Defendants. More succinctly, Defendants

are participating in rings that traffic in, make use of, and benefit from data stolen off of the Plaintiffs' and the Class members' wireless mobile devices.

338. On information and belief, Apple and certain of its App developers (including each Application Developer Defendant and the Unknown App Developers) combined and/or conspired to engage in a pattern of racketeering activity—*i.e.*, including those discussed above and engaging in unfair or deceptive practices in or affecting commerce in violation of 15 U.S.C. § 45 that knowingly facilitated and resulted in a stream of technologically-harmful App products coming to market that in essence turned an owner's otherwise functional iPhone, iPod, iPod Touch (or Android device) into a device that effectively eavesdrops on the device's owner by surreptitiously transmitting and broadcasting to others without permission the owner's private Address Book Data, as alleged herein—in violation of 18 U.S.C. § 1962(d). The Defendants have directly and indirectly receive income from these patterns of activities.

### **COUNT I**

#### **NEGLIGENCE & GROSS NEGLIGENCE - *RES IPSA LOQUITUR* & NEGLIGENCE *PER SE* (DUTIES OF CARE MANDATED BY CONTRACTS AND BY CRIMINAL STATUTES)**

339. Plaintiffs re-allege the above paragraphs.

340. iOS- and Android- App developers are generally subject to duties of care toward the users of their products that are contractually mandated by Apple, Google and Amazon.com in their respective App Store, Android Market and Android Appstore developer agreements and policies, as cited above. Specifically, the App developers,

including Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab (and the Unknown App Developers) have a duty to ensure that their Apps and their App-related conduct and services: (a) respect the privacy rights of App users, (2) do not access, upload or share data about or owned by a user—especially personal information or Address Book Data-type information maintained on the user’s wireless mobile device—without prior effective consent from the user following a clear and thorough explanation and disclosure of how the user’s data will be used and to whom it will be disclosed.<sup>60</sup>

341. As discussed above, various criminal statutes also prevent parties from accessing, transferring, manipulating, uploading, copying, storing and/or using another’s computes and electronic or computer data without prior permission. *See supra*. These laws set additional thresholds for the minimal duty of care that an Application Developer Defendant must meet with regard to their services and the Apps that they develop, market, distribute and sell to customers and users.

342. The Application Developer Defendants are obliged to abide by both of these fairly benign and customary statutory and contractual duties, which boil down to

---

<sup>60</sup> *See supra*, e.g., Apple’s App Store Guidelines at 17.1 – 17.2 and Google’s Android Market Developer Distribution Agreement at 4.3 – 4.4. Though Apple would apparently prefer that its customers be subject to a “caveat emptor” world, Apple nevertheless has common law and other duties to ensure that Apps validated (supposedly), approved, publicized and promoted by it and distributed through Apple’s AppStore specifically for the installation on iPhone, iPad and iPod Touch devices that Apple manufactures and sells—including the Apps of the Application Developer Defendants and the Unknown App Developers—meet its own specified and posted minimal standards, too.

the following principal: Don't use or take someone else's address book data from his or her iPhone, iPad or iPod Touch or Android device without that person's express prior consent.

343. Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab (and the Unknown App Developers) did not adhere to these specified standards of care. Their failures to adhere to the customary standard of care was not inadvertent. Instead, the Apps each contain expressly prohibited operations and functions—notably, the ability to surreptitiously harvest and upload to the respective Application Developer Defendant's computers and servers some or all of the App users' Address Book Data stored on their wireless mobile devices without the user's knowledge or permission. On information and belief, Apple knew or should have known that these Apps had Address Book Data-harvesting functionalities and lacked appropriate user-input permission sequences for the pre-approval of any use of the owner's Address Book Data.

344. Accordingly, Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab have not met the standard of care owed to the Plaintiffs and the members of the Class who acquired their Apps .

345. Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab also had and continue to have a duty to exercise reasonable care in safeguarding and protecting from disclosure the Plaintiffs' and the Class members' private Address Book Data stored on their wireless mobile devices.

346. Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab violated their respective duties by failing to either exercise reasonable care and safeguard and protect Plaintiffs' and the Class members' private Address Book Ddata.

347. Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLabs' conduct was reckless and wanton.

348. As a result of their noncompliance with the specified standards of care, Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab each disclosed and disseminated to themselves (and, on information and belief, to others) some or all of Plaintiffs' and the Class members' Address Book Data and the unaggregated information included therein.

349. It was reasonably foreseeable that Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik

Interactive, Rovio and ZeptoLabs' (and each of the Unknown App Developers') reckless failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class members' private Address Book Data would result in harm to the Plaintiffs and the Class members and in unauthorized third parties (including the Application Developer Defendants) gaining access to the Plaintiff' and the Class members' information for no lawful or authorized purpose.

350. Had Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab reasonably complied with their mandated standards of care—or had Apple simply enforced these self-adopted standards—Plaintiffs' and the Class members' Address Book Data would not have been improperly disclosed, disseminated and taken or otherwise exposed and compromised by Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab.

351. Plaintiffs and the class members have suffered legally recognizable actual harm as a result of this breach of the Defendants' duties toward them.

352. Plaintiffs and the Class members were damaged as a direct and/or proximate result of Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLabs' wrongful acquisition of and failure to protect their users' private Address

Book Data. Plaintiffs' and the Class members' recoverable damages include, *inter alia*, reasonable expenses for each Plaintiff and Class member to remedy and prevent the security breaches exposed by the Application Developer Defendants' wrongful conduct, recoupment of the value of the data appropriated from their wireless mobile devices, and other economic and noneconomic harm—for which they are entitled to compensation.

353. The Defendants', including Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLabs', wrongful actions and/or inaction (as described above) constituted (and continue to constitute) negligence at common law, negligence *per se* and negligence under the doctrine of *res ipsa loquitor*.

**COUNT II**  
**INVASION OF PRIVACY AND SECLUSION & PUBLIC DISCLOSURE OF PRIVATE FACTS**

354. Plaintiffs re-allege the above paragraphs.

355. An invasion of privacy occurs when: (i) a defendant has intentionally intruded on the victim's solitude, seclusion or private affairs; and (2) the intrusion would be offensive to a reasonable person. *See Valenzuela v. Aquino*, 853 S.W.2d 512, 513 (Tex. 1993). *See also* CAL. CONST., art. I, § 1.

356. The private affairs of the Plaintiffs include the contents of their private address books and contact information-type data stored on their wireless mobile devices (i.e., the Address Book Data). This information is especially private: it



ordinarily reveals with whom the wireless device owner associates him or herself, identifies the device owner's circles of friends, business associates, and family, may contain contacts that the mobile device owner may not want publicly disclosed, sales leads, customer and client lists, and other similar information that reasonable people ordinarily understand to be private.

357. Published news articles from venerable publications such as the NEW YORK TIMES similarly recognize that:

*The address book in smartphones [is] where some of the user's most personal data is carried . . .*<sup>61</sup>

358. Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLabs' actions directed toward their respective App users' (including Plaintiffs' and Class members') private Address Book Data—most of which were: (a) in violation of criminal statutes, (b) in flagrant contravention of contractual developer obligations, and (c) far from the level of care being exercised on information and belief by the majority of other App developers—resulted in the public disclosure and taking of such private information.

359. Plaintiffs' and the Class members' private Address Book Data is not a matter of legitimate public concern. Consequently, publicizing, disseminating,

---

<sup>61</sup> See Nicole Peroth and Nick Bilton, *Mobile Apps Take Data Without Permission*, NEW YORK TIMES (online ed. at [www.nytimes.com](http://www.nytimes.com) and <http://bits.blogs.nytimes.com/2012/02/15/google-and-mobile-apps-take-data-books-without-permission/> Feb. 15, 2012) (emphasis added).

exposing or surreptitiously obtaining individuals' private Address Book Data maintained on their wireless mobile devices is and will continue to be regarded as *highly offensive* to reasonable people, especially where, as here, the commission of a crime (i.e., the illegal and unauthorized accessing of a computer and copying and use of its data) was necessary for the Application Developer Defendants to first acquire the Address Book Data and learn their contents before their dissemination of the information.

360. Plaintiffs and the Class members were (and continue to be) damaged as a direct and/or proximate result of Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive Rovio and ZeptoLabs' invasion of their privacy by the public disclosure of their private facts (*i.e.*, the contents of their private Address Book Data). Such damages include, *inter alia*, expenses for securing their wireless mobile devices from another similar invasion of privacy (for example, by the purchase and installation of a wireless mobile device security App), costs associated with re-securing and validating the data and procuring and verifying the removal, deletion and scrubbing of the data and data points from the Defendants' records, computers and social networking systems, out of pocket expenses, and other economic and non-economic harm—for which they are entitled to compensation.

361. Plaintiffs and the Class members are entitled to recover actual and nominal damages.

362. Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLabs' wrongful actions and/or inactions (as described above) constituted (and continue to constitute) invasions of Plaintiffs' and the Class members' privacy by disturbing their seclusion and publicly disclosing their private facts (*i.e.*, their private Address Bok Data). As a direct and proximate result, Plaintiffs and the Class members were harmed and suffered damages.

### COUNT III

#### TEXAS THEFT LIABILITY ACT (TEX. CIV. P & REM CODE § 134.001, ET SEQ)

363. Plaintiffs re-allege the above paragraphs.

364. As discussed above, each Application Developer Defendant has committed a series of thefts of property under TEX. PENAL CODE § 31.03. The aggregate value of property appropriated by each Application Developer Defendants in its series of thefts raises the violation to first degree felony level theft.

365. Plaintiffs and the Class members had a possessory interest in the above-identified property, which was unlawfully appropriated from them by Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and/or ZeptoLab.

366. Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and/or ZeptoLab are liable to Plaintiffs and the Class members under TEX. CIV. PRAC. & REM. CODE § 134.03. (Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and/or ZeptoLab are similarly liable to Plaintiffs and the Class members under CAL. PENAL CODE § 502(e) for violations of CAL. PENAL CODE § 502(c).)

367. Plaintiffs and the Class members sustained as a result of, and are entitled to recover from Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and/or ZeptoLab actual damages for each of these millions of thefts. TEX. CIV. PRAC. & REM. CODE § 134.04. On information and belief, the actual damages should be no less than the fair market value to acquire in an arms-length transaction the property appropriated (i.e., the value of the discrete contact data points contained in each App user's Address Book Data set).

368. Under the TTLA, each Plaintiff and each Class member is also entitled to recover from each Application Developer Defendant who has stolen any portion of the Address Book Data from his or her respective wireless mobile device(s) an additional sum as determined by the trier of fact of up to \$1,000 per separate instance of theft of Address Book Data from each respective individual.

369. Plaintiffs and the Class members are also entitled to recover their reasonable costs and attorneys' fees.

**COUNT IV**  
**COMMON LAW MISAPPROPRIATION**

370. Plaintiffs re-allege the above paragraphs.

371. As alleged herein, Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab have appropriated either in whole or in part the private data sets making up each Plaintiff's and each Class member's wireless mobile device's private Address Book Data.

372. Plaintiffs and the Class members expended substantial time and effort collecting the data points in, and over time assembling, their address books and Address Book Data.

373. On information and belief, Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive Rovio and ZeptoLab have now via their respective Apps automatically and with little effort harvested and swept into their computers systems and, on information and belief, into their businesses social networking systems and data networks, some or all of the data fields (and, in some instances, the entirety) of the Plaintiffs' and the Class members' individual and aggregate personal, private Address Book Data and used that data for their own purposes and to their own benefit in their businesses.

374. On information and belief, Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLabs' respective Apps and each of these defendant's integrated App-related services and computer systems regularly scanned their App users' wireless mobile devices for updated address book information, noted particular Address Book changes, and sent those changes back to the respective Application Developer Defendant's computer servers, databases and social networking systems.

375. Essentially, on the cheap and on the sly these defendants have impermissibly mined their App users' phones for contacts data, thereby obtaining an unjustified and inequitable free ride on Plaintiffs' and the Class members' prior efforts.

376. Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab have each been guilty of misappropriation and Plaintiffs and the Class Members have sustained and are entitled to recover their actual damages.

377. On information and belief and as exemplified herein, Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLabs' conduct has been intentional and willful in nature and will continue unless enjoined by this Court.

378. Plaintiffs and the Class members have no adequate remedy at law.

**COUNT V**  
**CONVERSION**

379. Plaintiffs re-allege the above paragraphs.

380. Plaintiffs and the Class members have the immediate right to possession of, ownership of and/or title to their respective Address Book Data, which constitutes personal property. Plaintiffs' and the Class members' rights are superior to those of any Defendant or any other App developer.

381. As described herein, Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab have each wrongfully exercised dominion or control over at least a portion of the Plaintiffs' and the Class members' Address Book Data to the exclusion of, or inconsistent with, Plaintiffs' and the Class members' rights of exclusive possession and control.

382. Plaintiffs and the Class members have sustained actual losses and injuries as a natural and proximate result of these defendants' conversion of Plaintiffs' and the Class members' personal property.

383. On information and belief, these Defendants' conversion of Plaintiffs' and the Class members' personal property was knowing, willful, wanton and of a malicious nature and/or reckless, entitling Plaintiffs and the Class members to exemplary damages.

384. On information and belief, the Application Developer Defendants' wrongful conduct will continue unless enjoined by this Court.

385. Accordingly, Plaintiffs and the Class members seek their damages and injunctive relief for each of these Defendants' conversion of Plaintiffs' and the Class members' personal property.

386. Plaintiffs and the Class members have no adequate remedy at law.

**COUNT VI – CIVIL LIABILITY UNDER 18 U.S.C. § 1030(g)  
FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS**

387. Plaintiffs re-allege the above paragraphs.

388. On the basis of the Defendants' above alleged actions, Defendants Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab have each violated the requisite sections of 18 U.S.C. § 1030 so as to subject them under 18 U.S.C. § 1030(g) to civil liability and to permit recovery in a civil action by any person who suffers damage or loss by reason of the violation.

389. Plaintiffs and the Class members have suffered damage and/or loss by reason of each of these Defendants' violations of 18 U.S.C. § 1030.

390. Accordingly, Plaintiffs and the Class members seek recovery of their compensatory damages as authorized under 18 U.S.C. § 1030(g), including: (i) reasonable costs for validating the integrity of the Plaintiffs' and the Class members' Address Book Data and/or restoring such Address Book Data to the condition it was in



before the Defendants' respective offenses; (ii) costs for additional security measures to be put in place on the Plaintiffs' and the Class members' wireless mobile devices to remedy the Address Book Data-related security flaws that the Defendants have exposed and to inhibit and prevent similar offenses in the future; (iii) the reasonable costs for each Plaintiff and each Class member to conduct or have conducted a detailed damage assessment of his or her wireless mobile device and the Address Book Data contained thereon and to assess whether the Address Book Data and/or its availability or accessibility or the wireless mobile device has been impaired in any way; and (iv) the value and costs of the wireless airtime that those Apps caused to be consumed while surreptitiously uploading any portion of a Plaintiff's or a Class member's' Address Book Data from his or her wireless mobile device.

391. On information and belief and as exemplified herein, the Application Developer Defendants' conduct has been intentional and willful in nature and will continue unless enjoined by this Court.

392. Plaintiffs and the Class members have no adequate remedy at law.

**COUNT VII**  
**RICO VIOLATIONS UNDER 18 U.S.C. §§ 1961 – 1964**

393. Plaintiffs re-allege the above paragraphs.

394. Violations of 18 U.S.C. §§ 1343 (wire fraud) and 2314 (transportation of stolen property) are designated predicate acts under the Racketeering Influence & Corrupt Organizations Act (18 U.S.C. § 1962, et seq.). *See* 18 U.S.C. § 1961(1).

395. As alleged above, defendants Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio and ZeptoLab have each committed violations of 18 U.S.C. §§ 1343 (wire fraud) and 2314 (transportation of stolen property).

396. On information and belief, once defendant Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio or ZeptoLabs' (and the Unknown App Developers') Apps are installed on a wireless mobile device, the Apps function, in part, to surreptitiously harvest and intercept electronic communications and data. Accordingly, the defendants' Apps identified herein essentially constitute "electronic communication intercepting devices" under 18 U.S.C. § 2512. *See also* TEX. PEN. CODE 16.02(d)(1) (prohibiting the manufacture, sale or distribution of electronic or other devices designed for the nonconsensual interception of wire electronic or oral communications).

397. The wire-tapping and transportation of stolen property activities of the Application Developer Defendants (and of the Unknown App Developers) — essentially, the innumerable and surreptitious App-enabled thefts and unauthorized transmissions and use of millions of wireless device owners' Address Book Data ripped

from their wireless mobile devices—was facilitated by and committed as described herein with the knowing assistance, encouragement and participation of Apple in direct contravention of Apple’s own standards, policies, agreements, App validation & testing procedures and representations to the consumer market. Apple—who in its own sole discretion can decide whether to release or not release an App to the iOS wireless mobile device market and has the ability to disable or take down an App post-release—had and still has full visibility into each App’s code and functionality—including the Apps of each of the Application Developer Defendants (and the Unknown App Developers) —prior to the release of an App over Apple’s AppStore. (Notably, rather than rejecting, disabling or taking down the Instagram App complained of herein—which for all of 2011 surreptitiously harvested the Instagram App users’ Address Book Data—Apple instead named that App as its 2011 “App of the Year.”).

398. Each Application Developer Defendant (and each Unknown App Developer) in conjunction with Apple conducted or participated in the conduct of the affairs of an enterprise engaged in interstate commerce through a pattern of racketeering activity—here, numerous repeated instances of wire-tapping and transportation of stolen property as well as innumerable felony-level violations of Plaintiffs’ and the Class members’ personal computers and data—in violation of 18 U.S.C. § 1962(c). Each of the Application Developer Defendants (and each of the Unknown App Developers), in conjunction with Apple, have formed and participate in

an enterprise or association via the App-approval process and the AppStore distribution network and the affiliation of those companies that are and have been engaged in a pattern of racketeering activities. Moreover, they have pursued the common purpose of making money, gaining market-share, plugging additional persons, nodes and cross-links into their social networks, and expanding their networked databases illegally via the promotion, distribution and sale in interstate commerce of goods and services—*i.e.*, the offending Apps—that have Trojan-horse features that automatically and surreptitiously make use of users’ wireless mobile devices and that intercept and steal users’ personal Address Book Data and similar information in violation of 18 U.S.C. §§ 1030, 1343 and 2314 (and possibly 2512). This association exists separate and apart from the pattern of racketeering that is being pursued by these defendants.

399. Each Application Developer Defendant also directed and controlled the illegal conduct described herein and Apple was involved in and directed and controlled the management of the enterprise itself—the AppStore and its associated App development and distribution network.

400. Plaintiffs and the Class member have been directly harmed as a result of these Defendants’ violations of 18 U.S.C. § 1962. Accordingly, Plaintiffs and the Class member is entitled to recover treble damages and attorneys’ fees under 18 U.S.C. § 1964.

401. On information and belief and as exemplified herein, the Defendants' conduct has been intentional and willful in nature and will continue unless enjoined by this Court.

402. Plaintiffs and the Class members have no adequate remedy at law.

**COUNT VIII – INTERCEPTION OF ELECTRONIC COMMUNICATIONS UNDER  
18 U.S.C. §§ 2511 & 2520 OF THE ELECTRONIC COMMUNICATION PRIVACY ACT (“ECPA”)**

403. Plaintiffs re-allege the above paragraphs.

404. Section 2511 of the ECPA provides in part:

(1) [A]ny person who—

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire [ ] or electronic communication;

\* \* \*

(d) intentionally uses, or endeavors to use, the contents of any wire [or] electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire [ ] or electronic communication in violation of this subsection; . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

*See* 18 U.S.C. § 2511 (emphasis added).

405. Section 2520 of the ECPA further provides that:

(a) In General. [A]ny person whose wire [ ] or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity . . . which engaged in that violation such relief as may be appropriate.

(b) Relief.— In an action under this section, appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Computation of Damages.—

\* \* \*

(2) In any other action under this section, the court may assess as damages whichever is the greater of—

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000.

18 U.S.C. § 2520.

406. Each Defendant is a “person” within the meaning of § 2511.

407. Each Application Developer Defendant's respective App used to transfer information constitutes an “electronic device” under § 2510(5) and all other relevant federal and state statutes cited herein.

408. Each Plaintiff's (and each Class member's) sending of Address Book Data to his or her wireless mobile device from another computer via the electronic “syncing” process constitutes an “electronic communication” within the meaning of § 2510(12), as does any subsequent transmission or upload of any portion of the Address Book Data from the wireless mobile device.

409. On information and belief and as alleged herein, each Application Developer Defendant has without authorization intentionally intercepted electronic communications that contained some or all of the Address Book Data from users' wireless mobile devices and has intentionally made use of the content of such

communications. On information and belief, one or more of the Application Developer Defendants have also without authorization subsequently disclosed to others the contents such intercepted communications—such as through the sale or disclosure of assembled contact lists—in violation of 18 U.S.C. § 2511(c).

410. On information and belief, each such defendant knew or had reason to know that the information was obtained through the interception of a wire or electronic communication in violation of this statute.

411. Accordingly, each Plaintiff and each Class member is a “person whose . . . electronic communication [was] intercepted, disclosed or intentionally used in violation of this chapter” within the meaning of § 2520.

412. The Plaintiffs and the Class members have been directly harmed and suffered actual damages as a result of the Application Developer Defendants’ violations of the Electronic Communications Privacy Act.

413. Each Application Developer Defendant has benefited and profited as a result of their respective violations of the Electronic Communications Privacy Act and through their use of some or all of the Plaintiffs’ and the Class members’ Address Book Data contained in the intercepted communications.

414. On information and belief, the Application Developer Defendants have repeatedly and on a daily basis routinely violated the Electronic Communications Privacy Act in this manner since the launch of each of their respective Apps.

415. Accordingly, each Plaintiff and each Class member is entitled to recover from each respective Application Developer Defendant the greater of (i) his or her actual damages plus any Application Developer Defendant's profits realized from the use of his or her Address Book Data; or (ii) statutory damages of the greater of \$10,000 apiece or \$100 a day for each day of violation.

416. Plaintiffs and the Class members are also entitled to recover reasonable attorneys' fees and other litigation costs.

417. On information and belief and as exemplified herein, the Application Developer Defendants' conduct has been intentional and willful in nature and will continue unless enjoined by this Court. Accordingly, Plaintiffs and the Class members are also entitled to statutory punitive damages under 18 U.S.C. § 2520(b)(2).

418. Plaintiffs and the Class members are further entitled to preliminary and permanent equitable and declaratory relief.

419. Plaintiffs and the Class members have no adequate remedy at law.

**COUNT IX**  
**CIVIL LIABILITY FOR VIOLATIONS OF THE TEXAS WIRETAP ACT**<sup>62</sup>

420. Plaintiffs re-allege the above paragraphs.

---

<sup>62</sup> See also CAL. PENAL CODE § 502(e)(1) (authorizing a civil recovery of compensatory damages for the unauthorized access, copying or use of another's computer or computer data) and § 637.2 (authorizing civil actions for each victim of eavesdropping or wire tapping under CAL. PENAL CODE §§ 631 or 632 to recover from the violator a monetary award of the greater of \$5,000 or three times actual damages).



421. Each Application Developer Defendant's respective App constitutes an "electronic, mechanical or other device" within the meaning of TEX. CODE CRIM. PROC. art. 18.20, § 1(3) and TEX. PEN. CODE § 16.02(a).

422. The Application Developer Defendants' intentional interception, disclosure and use of the contents of electronic communications containing Plaintiffs' and the Class members' Address Book Data, as described above, constitute violations of TEX. PEN. CODE § 16.02(b) (the Texas Wiretapping Act).

423. Art. 18.20, § 16 of the Texas Code of Criminal Procedure provides as follows:

Art. 18.20. INTERCEPTION AND USE OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS.

Recovery of Civil Damages Authorized

Sec. 16. (a) A person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of this article, or in violation of Chapter 16, Penal Code, has a civil cause of action against any person who intercepts, discloses, or uses . . . the communication and is entitled to recover from the person:

- (1) actual damages but not less than liquidated damages computed at a rate of \$100 a day for each day of violation or \$1,000, whichever is higher;
- (2) punitive damages; and
- (3) a reasonable attorney's fee and other litigation costs reasonably incurred.

424. Plaintiffs and the Class members were harmed by the Application Developer Defendants' conduct allege herein.

425. Accordingly, under TEX. CODE CRIM. PROC. art. 18.20, § 16(a) each Plaintiff and each Class member is statutorily entitled to recover from each respective Application Developer Defendant who has harmed him or her **no less than the greater**

of: (i) his or her actual damages; or (ii) statutory liquidated damages of the greater of \$1,000 apiece or \$100 a day for each day of violation.

426. Plaintiffs and the Class members are also entitled to recover their reasonable attorneys' fees and other litigation costs.

427. On information and belief and as exemplified herein, the Application Developer Defendants' conduct has been intentional and willful in nature and will continue unless enjoined by this Court. Accordingly, Plaintiffs and the Class members are also entitled to statutory punitive damages under TEX. CODE CRIM. PROC. art. 18.20, § 16(a)(3).

**COUNT X**  
**AIDING AND ABETTING**

428. Plaintiffs re-allege the above paragraphs.

429. Apple receives substantial financial, economic, public relations and other benefits from its sale and distribution of the Apps identified in this Complaint.

430. Apple encourages persons to create Apps for distribution over its AppStore to iPhone, iPad and iPod Touch users (including Plaintiffs and members of the Class).

431. Apple provided the following material support and assisted and helped in the creation, marketing and distribution of the Application Developer Defendants' respective Path, Twitter, Facebook, Yelp!, Instagram, Foursquare, Gowalla, Beluga,

Foodspotting, Hipster, LinkedIn, Kik Messenger, Angry Birds and Cut the Rope Apps (and the Unknown App Developers' Apps) as described above and further by:

- a. providing on its websites online tutorials, APIs and code for creating Apps for its iPhones, iPads and iPods and providing other developer tools and toolkits;
- b. validating the functionality of each Application Developer Defendant's respective App;
- c. permitting each Application Developer Defendant to join Apple's iOS developer program and providing a consumer market of potential iOS App purchasers and users to each Application Developer Defendant via Apple's AppStore;
- d. posting, promoting and marketing over its AppStore each Application Developer Defendant's respective App (and subsequent versions and updates for each App) and storing each App and the code underlying each App on its servers;
- e. distributing each Application Developer Defendant's respective App over its AppStore and, via its AppStore, initiating, controlling and managing every single download of each Application Developer Defendant's App to each user's iPhone, iPad or iPod Touch wireless mobile devices; and,

f. collecting and paying to the Application Developer Defendants their cut of any revenues received relating to their Apps or for iAds running on those Apps.

432. Prior to their release on Apple's AppStore, Apple on information or belief knew or should have known that address book scanning and uploading functionality was included in the following Apps: Path, Twitter, Facebook, Yelp!, Instagram, Foursquare, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Messenger, Angry Birds and Cut the Rope (and the Apps of the Unknown App Developers).

433. Prior to their release on Apple's AppStore, Apple on information or belief knew or should have known that the following Apps were designed to and would be uploading at least portions of the App users' Address Book Data and would not require a user to grant explicit permission (via, for example, a proper dialogue permission box) prior to the App doing so: Path, Twitter, Facebook, Yelp!, Instagram, Foursquare, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Messenger, Angry Birds and Cut the Rope (and the Apps of the Unknown App Developers).

434. Before February of 2012, Apple never instructed Path, Twitter, Facebook, Yelp!, Burbn, Instagram, Foursquare Labs, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Interactive, Rovio or ZeptoLab to include any privacy-related user permission dialogue boxes in any of the Apps mentioned in this Complaint.

435. Apple's encouragement, assistance and support of each Application Developer Defendant was a substantial factor leading to the above-described harms inflicted upon the Plaintiffs and the Class members. If not for Apple's assistance, encouragement and support, the defendants' Trojan-horse-like Apps would never have been available to the iOS-device user marketplace over the AppStore and, thus, would never have been able to harm the Plaintiffs or other Class members who own and use iOS-based wireless mobile devices.

436. Since their introduction and through February 1, 2012, the following Apps did not comply with Apple's own user data privacy policies mandated in Apple's standard iOS developer agreements: Path, Twitter, Facebook, Yelp!, Instagram, Foursquare, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Messenger, Angry Birds and Cut the Rope.

437. Apple breached its own self-established App-related standard of care when it posted each of the non-conforming Apps identified in this Complaint for sale and distribution over the AppStore and then initiated downloads of these non-conforming Apps to unsuspecting iPhone, iPad and iPod Touch owners.

438. Apple never disclosed to iPhone, iPad or iPod Touch owners that the non-conforming Path, Twitter, Facebook, Yelp!, Instagram, Foursquare, Gowalla, Beluga, Foodspotting, Hipster, LinkedIn, Kik Messenger, Angry Birds or Cut the Rope Apps that Apple offered over its AppStore each had the capability to and, in fact, would

access, upload and/or remotely store at least a portion of the device owner's Address Book Data before seeking explicit permission from the device owner to do so.

439. Accordingly, Apple knowingly or recklessly aided and abetted each Application Developer Defendant in the commission of the wrongful activities described above and, consequently, is jointly and severally liable to the Plaintiffs and the Class members on each of the claims and for all of the harm and damages described herein.

**COUNT XI**  
**UNJUST ENRICHMENT**

440. Plaintiffs re-allege the above paragraphs.

441. The Defendants have been unjustly enriched by their wrongful actions described above.

442. Defendants have retained the benefits and profits that they obtained and realized from their unauthorized acquisition, uploading, interception, and use of Plaintiffs' and the Class members' Address Book Data. As of yet, Defendants have not fully purged or disgorged their computer systems, databases or social networks of information, data nodes and coupled data links originally taken or gleaned from Plaintiffs' and the Class members' surreptitiously obtained Address Book Data.

443. On information and belief, the Application Developer Defendants benefited from their unauthorized acquisition, uploading and use of Plaintiffs' and the Class members' Address Book Data. On information and belief, their use of the

individuals' Address Book Data helped facilitate the rapid and exponential growth of each of their respective social networking databases and services or gaming platforms. By doing so, they further enhanced the overall economic value of each of their respective organizations and business operations for fundraising, advertising and other purposes.

444. On information and belief, one or more of the Defendants have also re-sold to others for value portions of the Address Book Data wrongfully obtained from Plaintiffs and the Class members. Those Defendants have retained or made use of the proceeds of any such sales.

445. On information and belief, the Application Developer Defendants and Apple have also received revenues and other benefits associated with their distribution and/or sales of the non-conforming Apps identified herein.

446. As a result of the Defendants' wrongful conduct described herein, each Defendant has received, directly or indirectly, funds and other valuable benefits which each company was not rightfully or equitably entitled to in an amount to be determined at trial, and has been unjustly enriched thereby.

## **COUNT XII**

### **CONSTRUCTIVE TRUST**

447. Plaintiffs re-allege the above paragraphs.

448. On information and belief, the Defendants have inequitably profited from their wrongful activities described herein and have been unjustly enriched by their wrongful actions described above.

449. To protect Plaintiffs' and the Class members' rightful interests, Plaintiffs and the Class members are entitled to and the Defendants' actions necessitate the imposition of a constructive trust over all funds and benefits (or the proceeds thereof) wrongfully received or obtained by the Defendants in connection with or derived from either their wrongful access, interception and/or use of Plaintiffs' and the Class Members' Address Book Data and/or wireless mobile devices, the sale or distribution of the non-conforming Apps, or on account of their other wrongful activities described herein.

450. To prevent further immediate and irreparable harm, the Court should immediately enjoin any disposition by Defendants of any such funds or valuable benefits.

451. On information and belief, a non-negligible portion of each Application Developer Defendant's current social networking database (including, for example, contacts, data, nodes and connections and cross-links between nodes) consists of or was gleaned or derived from Plaintiffs' and the Class members' Address Book Data.

452. On information and belief, the value of social networking companies—including several of the Application Developer Defendants—is based upon and roughly



proportional to the overall size of their respective social networking databases. Thus, the defendants' own business value has been enhanced by the use and inclusion of Plaintiffs' and the Class members' Address Book Data in the defendants' operational social networking databases and, on information and belief, has accelerated and helped facilitate the exponential growth of the defendants' networks and businesses.

453. Accordingly, to protect Plaintiffs' and the Class members' rightful interests and to prevent the unjust and inequitable enrichment of the defendants, the Application Developer Defendants' actions necessitate the imposition of a constructive trust over: (i) a percentage to be determined at trial of each Application Developer Defendant's outstanding equity on a fully-diluted basis and any proceeds from any sale thereof; and (ii) a percentage to be determined at trial of the gross proceeds received or promised on any sale or disposition of the equity or operational business segment of any Application Developer Defendant.

454. The Plaintiffs and the Class members are entitled to immediate, temporary, preliminary and permanent injunctive relief.

455. To protect consumers' privacy and to prevent further immediate and irreparable harm to the Plaintiffs, the Class members and to wireless mobile device consumers as a whole, the Court should immediately (a) direct Apple to actually enforce against all App developers the user-data-privacy provisions contained in Apple's App development agreements and policies; and (b) enjoin Apple from

initiating any further downloads to others of Apps (including those identified herein) that (i) transmit and/or upload in unencrypted form any portion of the App user's Address Book Data, or (ii) have data-uploading functionality and access any portion of the App users' Address Book Data in advance of the confirmation of explicit permission to do so from the device owner.

### **RELIEF**

457. **INJUNCTIVE RELIEF.** Plaintiffs and Class members are entitled as alleged herein to immediate, temporary, preliminary and permanent injunctive relief, including the following:

- (i) an order prohibiting the distribution or operation of Apps having coding and/or functionalities that can or do cause the unencrypted uploading of any portion of a wireless mobile device owner's Address Book Data prior to the owner granting explicit, knowing permission for the upload and any subsequent use of such data;
- (ii) an order prohibiting any non-authorized use of Plaintiffs' and the Class members' Address Book Data and requiring the return and/or deletion from Defendants' computers and computer systems—as verified by an independent third party data security company— of any wrongfully obtained portions of Plaintiffs' and the Class members' Address Book Data as well as any data, data nodes or data connections derived therefrom;
- (iii) an order requiring Defendants to submit to periodic compliance audits by an independent third party data security company regarding the privacy and security of wireless mobile device users' Address Book Data and the handling of any such data that may come into Defendants' possession, custody or control;
- (iv) an order enjoining Defendants' violations of any of the criminal laws cited herein;

(v) an order mandating that Apple provide its iOS wireless mobile device users with a built-in option for the encrypted storage of their Address Book Data on their iOS- devices; and,

(vi) an order directing the Defendants to preserve and maintain throughout the course of this proceeding all evidence pertaining to this matter—including computer and electronic records, historical App code, and records relating to attempts to access the wireless mobile device of any Plaintiff or Class member or to subsequently upload, copy, use or disseminate any portion of any Plaintiff's or Class member's Address Book Data.

All conditions precedent to Plaintiffs' and the Class members' claims for relief have been performed and/or occurred.

458. **DAMAGES.** As a direct and/or proximate result of the Defendants' wrongful actions and/or inaction (as described above), Plaintiffs and the Class members suffered (and continue to suffer) damages as alleged above, including expenses for verifying the integrity of and/or repairing their Address Book Data; expenses for verifying the security and integrity of (and/or repairing) their wireless mobile devices; expenses for obtaining and installing additional appropriate security products to prevent further wrongful access or use of their wireless mobile devices and Address Book Data; loss of privacy; diminution or loss of Address Book Data value; loss of the wireless airtime and wireless mobile device computational, processing and battery power and life consumed during the unauthorized uploading and data transfer of users' Address Book Data; out of pocket expenses; and other economic and noneconomic harm—for which they are entitled to compensation. Plaintiffs and the

Class members also are each entitled to recover nominal damages and the following **statutory damages**:

- liquidated damages under TEX. CODE CRIM. PROC. art. 18.20, § 16(a) of *no less than the greater of* \$1,000 or \$100 a day for each day of violation from each respective Application Developer Defendant who has harmed him or her;
- any Application Developer Defendant's profits realized from the unauthorized use or dissemination of the Plaintiff's or the Class member's Address Book Data or unauthorized accessing of Plaintiff's or the Class member's wireless mobile device, under 18 U.S.C. § 2520;
- statutory damages of no less than the greater of \$10,000 or \$100 a day for each day of violation under 18 U.S.C. § 2520 from each respective Application Developer Defendant who has harmed him or her; and,
- additional damages under TEX. CIV. PRAC. & REM. CODE § 134.005(a)(1) of up to \$1,000 (as determined by the trier of fact) for each separate instance of theft of any portion of a Plaintiff's or Class member's Address Book Data by an Application Developer Defendant.

Plaintiffs' and the Class members' damages were foreseeable by the Defendants and exceed the minimum jurisdictional limits of this Court. All conditions precedent to Plaintiffs' and Class members' claims have been performed and/or occurred.

459. **TREBLE DAMAGES.** Plaintiffs and the Class members also are entitled under 18 U.S.C. § 1964(c) to recover treble damages for their injuries suffered by reason of Defendants' intentional and wrongful acts constituting violations of 18 U.S.C. § 1964(c).

460. **EXEMPLARY AND PUNITIVE DAMAGES.** Plaintiffs and the Class members also are statutorily and otherwise entitled to recover exemplary and punitive

damages, as specified herein, as punishment and to deter such wrongful conduct in the future.

461. **EQUITABLE RELIEF.** To prevent the unjust enrichment of the Defendants, Plaintiffs and the Class members are also entitled to equitable relief, including an award of and/or the imposition of a constructive trust over (i) any profits or benefits Defendants received, obtained or realized from their from wrongful access of Plaintiffs' or the Class members' wireless mobile devices and/or use of any portion of their Address Book Data; and (ii) to compensate for the accelerated growth of certain Application Developer Defendants' social networks and overall business via the use of portions of Plaintiffs' and the Class members' Address Book Data, a percentage to be determined at trial of (a) each such Application Developer Defendant's outstanding equity on a fully-diluted basis and any proceeds from any sale thereof; and (b) the gross proceeds received or promised on any sale or disposition of the equity or operational business segment of any such Application Developer Defendant.

462. **ATTORNEYS' FEES, LITIGATION EXPENSES AND COSTS.** Plaintiffs and the Class members also are entitled to recover their attorneys' fees, litigation expenses and court costs in prosecuting this action and these claims.

#### **PRAYER**

Accordingly, Plaintiffs, on behalf of themselves and the Class Members, respectfully request that: (a) Defendants be cited to appear and answer this lawsuit, (b)

this action be certified as a class action, (c) Plaintiffs be designated the Class Representatives, (d) Plaintiffs' counsel be appointed as Class Counsel, and (e) immediate, temporary and preliminary relief be provided as requested above. Plaintiffs, on behalf of themselves and the Class members, further request that upon final trial or hearing, judgment be awarded against Defendants, in favor of Plaintiffs and the Class members, for:

(i) actual, compensatory, incidental, consequential, statutory, and/or nominal damages (as described above) and an award of Defendants' wrongfully obtained profits;

(ii) statutory treble damages;

(iii) exemplary and punitive damages (as described above and as statutorily authorized);

(iv) injunctive relief as set forth above;

(v) imposition of a constructive trust as described herein and disgorgement of any benefits wrongfully received or obtained by the Defendants;

(vi) pre- and post-judgment interest at the highest applicable legal rates;

(vii) attorneys' fees and litigation expenses incurred through trial and any appeals;

(viii) costs of suit;

(ix) an order under 11 U.S.C.S. § 523(a)(6) that Defendants be prohibited from any discharge under 11 U.S.C.S. § 727 for injuries caused to Plaintiffs' and the Class members by Defendants' malicious and willful conduct, and,

(x) such other and further relief that this Court deems just and proper.

**JURY DEMAND**

Plaintiffs, on behalf of themselves and the Class members, request a jury trial on all issues triable in this action.

Respectfully submitted,

THE EDWARDS LAW FIRM

A handwritten signature in black ink, appearing to read "Jeff Edwards", with a long, sweeping horizontal line extending to the right.

By: \_\_\_\_\_  
Jeff Edwards  
State Bar No. 24014406  
THE BREMOND HOUSTON HOUSE  
706 GUADALUPE  
Austin, Texas 78701  
Tel. 512-623-7727  
Fax. 512-623-7729  
[jeff@edwards-law.com](mailto:jeff@edwards-law.com)

Carl F. Schwenker  
Texas Bar No. 00788374  
LAW OFFICES OF CARL F. SCHWENKER  
The Bremond-Houston House  
706 Guadalupe Street  
Austin, Texas 78701  
Tel. (512) 480-8427  
Fax (512) 857-1294  
[cfslaw@swbell.net](mailto:cfslaw@swbell.net)

Dirk Jordan  
Texas Bar No. 00784359  
*Jordan Law Firm*  
The Bremond-Houston House  
706 Guadalupe Street  
Austin, Texas 78701  
512-551-0669  
512-551-0668 fax  
[dirk@dirkjordan.com](mailto:dirk@dirkjordan.com)

ATTORNEYS FOR THE PLAINTIFFS  
AND THE PUTATIVE CLASS