

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

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

**OSCAR HERNANDEZ, individually and on
behalf of a class of similarly situated
individuals,**
Plaintiffs,
vs.
PATH, INC.,
Defendant.

Case No.: 12-CV-01515 YGR
**ORDER GRANTING IN PART MOTION TO
DISMISS WITH LEAVE TO AMEND**

Plaintiff Oscar Hernandez brings this putative class action against Defendant Path, Inc. (“Path”) alleging that after putative class members downloaded Path’s “App” to their mobile devices, that Path accessed the putative class members’ mobile devices and uploaded to its servers the class members’ personally identifiable information, including the address book stored on the mobile devices, and shared this information with advertisers. Plaintiff’s First Amended Complaint (“FAC”) alleges ten claims: (1) Violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*; (2) Violations of the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*; (3) Violations of the California Computer Crime Law, California Penal Code § 502; (4) Violations of California’s Invasion of Privacy Act, California Penal Code § 630 *et seq.*; and state law claims for (5) Violations of the California Unfair Competition Law, California Business and Professions Code § 17200 *et seq.*; (6) Invasion of Privacy and Seclusion and Public Disclosure of Private Facts; (7) Negligence; (8) Conversion; (9) Trespass to Personal Property/ Chattel; and (10) Unjust Enrichment.

Defendant Path moves to dismiss Counts III through X for lack of subject matter jurisdiction on the grounds that Plaintiff has not alleged Article III standing; and moves to dismiss all claims

1 pursuant to Rule 12(b)(6) for failure to state a claim upon which relief can be granted. The Court
2 heard oral argument on July 31, 2012.

3 Having carefully considered the papers submitted, the pleadings in this action, and the oral
4 argument of counsel, for the reasons set forth below, the Court hereby **GRANTS IN PART** the Motion
5 to Dismiss **WITH LEAVE TO AMEND**.

6 **I. BACKGROUND**

7 Path operates a social networking-enabled photo sharing and messaging service for wireless
8 mobile devices. Plaintiff seeks to represent a class of users that downloaded the Path App to their
9 mobile device. When the users downloaded the Path App, Path accessed, uploaded and stored data
10 from the users' Contact Address Books.¹ According to the FAC, the Path App also installed tracking
11 software onto the users' mobile devices that enabled Path to track user interactions on social
12 networking websites, including geo-tagging GPS coordinates within digital content, such as
13 photographs and videos. Plaintiff further alleges that Path is storing this information on its servers
14 without encryption, which presents a security risk.

15 **II. STANDING**

16 Because standing is a threshold jurisdictional question, the Court will address that issue first.
17 *See Steel Company v. Citizens for a Better Environment*, 523 U.S. 83, 94, 102 (1998).

18 To establish Article III standing, a plaintiff must satisfy three elements: (1) "the plaintiff must
19 have suffered an injury in fact—an invasion of a legally protected interest which is (a) concrete and
20 particularized and (b) actual or imminent, not conjectural or hypothetical"; (2) "there must be a
21 causal connection between the injury and the conduct complained of"; and (3) "it must be likely, as
22 opposed to merely speculative, that the injury will be redressed by a favorable decision." *Lujan v.*
23 *Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992) (internal quotation marks, citations and footnote
24 omitted).

25
26
27 ¹ According to the FAC, "[a] contact address book is a database within a Mobile Device for storing entries
28 called 'contacts.' Each contact consists of a few standard fields of data, including but not limited to, contact
names, phone numbers, mailing addresses, e-mail addresses, instant message screen names, job title,
employer, websites, birthdays, and notes." (FAC ¶ 41.)

1 Plaintiff identifies three injuries to establish Article III standing: (1) diminished mobile
2 device resources, such as storage, battery life, and bandwidth; (2) increased, unexpected, and
3 unreasonable risk to the security of sensitive personal information; and (3) future costs to remove
4 embedded code from media files uploaded through the Path App.

5 (1) The specific harm caused by diminished resources of which Plaintiff complains is *de*
6 *minimus*: depletion of “two to three seconds of battery capacity.” (FAC ¶ 122.)²

7 (2) The hypothetical threat of future harm due to a security risk to Plaintiff’s personal
8 information is insufficient to confer Article III standing. *Krottner v. Starbucks Corp.*, 628 F.3d 1139,
9 1141-43 (9th Cir. 2010).

10 (3) Although Plaintiff has not alleged that he spent time or money removing the Path App
11 and associated tracking files, the harm alleged is not hypothetical. According to the FAC, the Path
12 App installed tracking software onto Plaintiff’s mobile device, Plaintiff wants to remove the tracking
13 software, and alleges that he would need to pay a trained technician as much as \$12,250.00³ to do so.
14 (See FAC ¶ 73). Thus, Plaintiff has sufficiently alleged that he has suffered an actual injury as a
15 result of Path’s actions.

16 Based on the foregoing analysis, the Court **DENIES** this basis for the Motion to Dismiss.

17 **III. RULE 12(b)(6) ANALYSIS**

18 **A. LEGAL STANDARD**

19 A motion to dismiss under Rule 12(b)(6) tests the legal sufficiency of the claims alleged in
20 the complaint. *Ileto v. Glock, Inc.*, 349 F.3d 1191, 1199-1200 (9th Cir. 2003). All allegations of
21 material fact are taken as true. *Johnson v. Lucent Techs., Inc.*, 653 F.3d 1000, 1010 (9th Cir. 2011).
22 To withstand a motion to dismiss, “a complaint must contain sufficient factual matter, accepted as
23

24 _____
25 ² Plaintiff argues that there are calculable injuries to his mobile device resources and the bandwidth for which
26 he pays to access the internet and calculable costs to draining bandwidth, memory and battery power. In a
27 footnote Plaintiff indicates that “discovery will allow Plaintiff the opportunity to quantify the amount [of
28 bandwidth] used by Path’s App.” (Opp’n 12, n.18.) Plaintiff should be able to determine the extent of his
injuries without the benefit of discovery.

³ Path disputes that removal of the embedded code would require a trained computer technician. According
to Path, removal is “a simple act requiring no more than two swipes of his finger on his phone.” On a motion
to dismiss, the Court must accept as true the well-pleaded allegation.

1 true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678
2 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 557 (2007)).

3 *1. Requests for Judicial Notice.*

4 Although review is generally limited to the contents of the complaint and documents
5 attached thereto, *Allarcom Pay Television. Ltd. v. Gen. Instrument Corp.*, 69 F.3d 381, 385 (9th Cir.
6 1995), the Court may also consider a matter that is properly the subject of judicial notice. *Lee v. City*
7 *of Los Angeles*, 250 F.3d 668, 688-89 (9th Cir. 2001). Under Federal Rule of Evidence 201, a court
8 may take judicial notice of a fact not subject to reasonable dispute because it is generally known
9 within the trial court’s territorial jurisdiction, or can be accurately and readily determined from
10 sources whose accuracy cannot reasonably be questioned. Fed. R. Evid. 201(b).

11 Defendant has requested the Court take judicial notice of a patent application, the Path App’s
12 pages on the iPhone App Store and Google Play store, the Apple App Store and Google Play
13 marketplace webpages, screenshots of the Path user-interface, and notices provided by the iOS and
14 Android OS. The Court will take judicial notice of the patent application because it is “capable of
15 accurate and ready determination by resort to sources whose accuracy cannot reasonably be
16 questioned.” However, the screenshots and webpages are not subject to judicial notice; information
17 contained on the screenshots, websites, and Path’s privacy policy are not from sources whose
18 accuracy cannot reasonably be questioned, nor are they facts generally known within the territorial
19 jurisdiction of this Court. *See* Fed. R. Evid. 201(b).

20 *2. Incorporation by Reference.*

21 Under the incorporation by reference doctrine, if “the plaintiff’s claim depends on the
22 contents of a document, the defendant attaches the document to its motion to dismiss, and the parties
23 do not dispute the authenticity of the document, even though the plaintiff does not explicitly allege
24 the contents of that document in the complaint,” the Court may consider the document without
25 converting the motion to dismiss into a motion for summary judgment. *Knievel v. ESPN*, 393 F.3d
26 1068, 1076 (9th Cir. 2005). The Court considers Path’s Privacy Policy, which was in place and
27 publicly available during the relevant class period (*see* Van Horn Dec. Ex. 1, Dkt. No. 16-2) to be
28 incorporated by reference into the FAC because Plaintiff references the privacy policy and Plaintiff’s

1 claims are based on how Path discloses information to users. *See Knieval, supra*, 393 F.3d at 1076.
2 The Court does not consider the remaining documents to be incorporated by reference in the FAC.
3 Although referenced by the FAC, Plaintiff’s claims do not depend on the contents of the referenced
4 documents.

5 **B. ANALYSIS OF PLAINTIFF’S CLAIMS**

6 Path argues Counts I and II fail to state a claim and that even if this Court had subject matter
7 jurisdiction over Counts III through X, each should be dismissed for failure to state a claim. The
8 Court analyzes the sufficiency of the allegations of each Count below.

9 *I. Count I – Federal Wiretap Act: 18 U.S.C. § 2511(1).*

10 The Electronic Communications Privacy Act, commonly known as the Federal
11 Wiretap Act, prohibits “intentionally intercepts, endeavors to intercept, or procures any other person
12 to intercept or endeavor to intercept, any wire, oral, or electronic communication.” 18 U.S.C. §
13 2511. According to the FAC, Path intercepted and procured Plaintiff’s and the Class Members’
14 electronic communications, which included procuring users’ contact address books, and intercepting
15 interactions between users and their contacts online from their Mobile Devices. (FAC ¶ 141.)

16 The FAC fails to allege that Defendant intercepted any communication contemporaneous
17 with its transmission. Although Path allegedly transmitted the Class Members’ Contact Address
18 Books from the Class Members’ mobile devices to Path’s servers, Path did not “intercept” a
19 “communication” to do so. Likewise, Plaintiff fails to allege facts to support an inference that Path
20 “intercepted” a “communication” on a third-party social network cite contemporaneous with, and
21 not after, the communication was posted on the social networking website.⁴

22 Based on the foregoing analysis, the Court **GRANTS** the Motion to Dismiss Count I. Out of an
23 abundance of caution that an “interception” as defined can, in fact, be alleged specifically, the Court
24 grants **LEAVE TO AMEND** to the extent this claim can be amended consistent with this Order.

25
26 _____
27 ⁴ The Federal Wiretap Act requires an intentional “intercept.” The common understanding of the term
28 intercept, *i.e.*, “to stop, seize, or interrupt in progress or course or before arrival,” is further defined by the
Federal Wiretap Act itself as “*the aural or other acquisition of the contents of any wire, electronic, or oral
communication through the use of any electronic, mechanical, or other device.*” Webster’s Ninth New
Collegiate Dictionary at 630 (1988); 18 U.S.C. § 2510(4) (emphasis supplied).

1 2. Count II – Stored Communications Act: 18 U.S.C. § 2701.

2 The Stored Communications Act (“SCA”) makes it an offense to “intentionally
3 access[] without authorization a facility through which an electronic communication service is
4 provided; or intentionally exceed[] an authorization to access that facility ... and thereby obtain[]
5 ... access to a wire or electronic communication while it is in electronic storage in such system.” 18
6 U.S.C. § 2701(a)(1). Plaintiff’s SCA claim fails on multiple fronts.

7 First, an “electronic communication service” is statutorily defined as a service which
8 provides its users the ability to send or to receive wire or electronic communications. 18 U.S.C. §
9 2510(15).⁵ “Existing telephone companies and electronic mail companies are providers of electronic
10 communication services.” S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.
11 Plaintiff is not a provider of electronic communication services and his iPhone is not a facility
12 through which such service is provided.

13 Second, as defined by and used in the SCA, the term “electronic storage” refers to the
14 temporary, intermediate storage of the electronic communication that is incidental to the electronic
15 transmission of the communication. As alleged in the FAC, the putative class members’ Contact
16 Address Books are not a communication to which the SCA applies.

17 Based on the foregoing analysis, the Court **GRANTS** the Motion to Dismiss Count II. Out of
18 an abundance of caution that these terms as defined can, in fact, be alleged specifically, the Court
19 grants **LEAVE TO AMEND** to the extent this claim can be amended consistent with this Order.

20 3. Count III – California Computer Crime Law: Cal. Penal Code § 502.

21 Plaintiff alleges that Path violated subsections 1, 2, 6, 7, and 8 of the California
22 Computer Crime Law, Cal. Penal Code §§ 502(c)(1), (2), (6)-(8). Those sections impose civil
23 liability upon any party who:

- 24 (1) “Knowingly accesses and without permission alters, damages, deletes, destroys, or
25 otherwise uses any data, computer, computer system, or computer network in order to either (A)
26 devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control
27 or obtain money, property, or data,” *id.* § 502(c)(1);

28

⁵ The SCA uses the definitions of terms defined in 18 U.S.C. § 2510. *See* 18 U.S.C. § 2711.

1 (2) “Knowingly accesses and without permission takes, copies, or makes use of any data
2 from a computer, computer system, or computer network, or takes or copies any supporting
3 documentation, whether existing or residing internal or external to a computer, computer system,
4 or computer network,” *id.* § 502(c)(2);

5 (3) “Knowingly and without permission provides or assists in providing a means of
6 accessing a computer, computer system, or computer network in violation of this section,” *id.* §
7 502(c)(6);

8 (4) “Knowingly and without permission accesses or causes to be accessed any computer,
9 computer system, or computer network,” *id.* § 502(c)(7); or

10 (5) “Knowingly introduces any computer contaminant into any computer, computer
11 system, or computer network,” *id.* § 502(c)(8). Subsection 502(b)(10) defines a “computer
12 contaminant” as “any set of computer instructions that are designed to modify, damage, destroy,
13 record, or transmit information within a computer, computer system, or computer network
14 without the intent or permission of the owner of the information.” *Id.* § 502(b)(10).

15 The parties dispute whether “without permission” as used in Cal. Penal Code § 502(c)(1), (2),
16 (6), and (7) means (i) unauthorized or (ii) unauthorized access that circumvents a technical or code-
17 based barrier. *See also Weingand v. Harland Fin. Solutions, Inc.*, C-11-3109 EMC, 2012 WL
18 2327660, at *4-6 (N.D. Cal. June 19, 2012) (discussing split of authority without deciding which
19 construction to adopt so as to allow complete briefing and factual development on motion for
20 summary judgment). The parties also dispute whether software code that is installed voluntarily is a
21 “computer contaminant,” which the statute limits civil liability to conduct “without the intent or
22 permission of the owner of the information.” *See* Cal. Penal Code § 502(b)(10). Based on the
23 current limited briefing, the Court cannot conclude as a matter of law whether Path’s alleged
24 conduct—*i.e.*, downloading the Path App, which Plaintiff voluntarily installed on his mobile device,
25 contained undisclosed software code that surreptitiously transferred data stored on Plaintiff’s mobile
26 device to Path’s servers—falls outside the scope of the California Computer Crime Law, Cal. Penal
27 Code § 502(c).

28 Based on the foregoing analysis, the Court **DENIES** the Motion to Dismiss Count III.

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

4. Count IV – California’s Invasion of Privacy Law: Cal. Penal Code §§ 630 et seq.

California Penal Code Section 631, captioned “Wiretapping,” provides, in part:

Any person who ... willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable ...

As set forth in the analysis of Count I for violation of the Federal Wiretap Act (*see* Section III.B.1, *supra*), Plaintiff fails to allege that Path intercepted a communication in transit. Cal. Penal Code § 631(a).⁶

Based on the foregoing analysis, the Court **GRANTS** the Motion to Dismiss Count IV. Out of an abundance of caution that an “interception” as defined can, in fact, be alleged specifically, the Court grants **LEAVE TO AMEND** to the extent this claim can be amended consistent with this Order.

5. Count V – California’s Unfair Competition Law: Cal. Bus. & Prof. Code §§ 17200 et seq.

California’s Unfair Competition Law (“UCL”) prohibits “any unlawful, unfair or fraudulent business act or practice.” Cal. Bus. & Prof. Code § 17200.

a) Unlawful Prong

To state a cause of action for an “unlawful” practice under the UCL, Plaintiff must allege the violation of some other law. *Cel-Tech Comm’ns, Inc. v. Los Angeles Cellular Telephone Co.*, 20 Cal. 4th 163, 180 (Cal. 1999). Plaintiff has adequately alleged unlawful conduct under Count III, which may serve as the predicate violation. The conduct alleged in the FAC, if true, constitutes an unlawful act or practice within the meaning of the UCL.

⁶ Both parties cite cases that have analyzed whether the federal Wiretap Act preempts California’s Invasion of Privacy Law. *Compare Bunnell v. Motion Picture Ass’n of America* 567 F. Supp. 2d 1148, 1154 (C.D. Cal. 2007) (California’s Invasion of Privacy Law is preempted) *with Leong v. Carrier IQ Inc.*, 2012 WL 1463313 (C.D. Cal. Apr. 27, 2012) *and Valentine v. NebuAd, Inc.*, 804 F. Supp. 2d 1022, 1028-29 (N.D. Cal. 2011) (California’s Invasion of Privacy Law is not preempted). Based on the current cursory briefing, which does not explain why the Court should adopt either party’s position on the issue of preemption, the Court is unable to determine whether this claim is preempted.

1 b) Unfair Prong

2 An act or practice is “unfair” when it “offends an established public policy or
3 when the practice is immoral, unethical, oppressive, unscrupulous or substantially injurious to
4 consumers.” *Smith v. State Farm Mutual Automobile Insurance Co.*, 93 Cal. App. 4th 700, 719 (Cal.
5 Ct. App. 2001). The conduct alleged in the FAC, if true, constitutes an unfair act or practice within
6 the meaning of the UCL.

7 c) Fraudulent Prong

8 A business practice is fraudulent under the UCL if members of the public are
9 likely to be deceived. *Sybersound Records, Inc. v. UAV Corp.*, 517 F.3d 1137, 1152 (9th Cir. 2008).
10 Plaintiff fails to allege fraud with particularity. *See Kearns v. Ford Motor Co.*, 567 F.3d 1120 (9th
11 Cir. 2009) (UCL claims that sound in fraud are subject to heightened pleading requirement of Rule
12 9(b)).

13 Nonetheless, Plaintiff has sufficiently pled two of the three prongs, which is sufficient to
14 withstand a motion to dismiss.⁷ Therefore, the Court **DENIES** the Motion to Dismiss Count V.

15 6. Count VI – State Common Law Privacy Torts.

16 The elements for a claim of Public Disclosure of Private Facts are: “(1) public
17 disclosure (2) of a private fact (3) which would be offensive and objectionable to the reasonable
18 person and (4) which is not of legitimate public concern.” *Shulman v. Group W Prods., Inc.*, 18 Cal.
19 4th 200, 214 (Cal. 1998). Public disclosure means “communicating it to the public at large, or to so
20 many persons that the matter must be regarded as substantially certain to become one of public
21 knowledge.” Cal. Jury Instr.–Civ. 7.21.

22 Plaintiff has not alleged a *public* disclosure, only that Path stored Plaintiff’s Contact Address
23 Book on its servers.

24 Based on the foregoing analysis, the Court **GRANTS** the Motion to Dismiss Count VI. Out of
25

26 ⁷ Federal Rule of Civil Procedure 12(b)(6) is not an appropriate device to eliminate a portion of a claim.
27 *SocialApps, LLC v. Zynga, Inc.*, 4:11-CV-04910 YGR, 2012 WL 381216, at *2 (N.D. Cal. Feb. 6, 2012)
28 (“motion under Rule 12(b)(6) may not be used to challenge only certain allegations within a claim”) (citing
Thompson v. Paul, 657 F. Supp. 2d 1113, 1129 (D. Ariz. 2009)).

1 an abundance of caution that a “public disclosure” can, in fact, be alleged specifically, the Court
2 grants **LEAVE TO AMEND** to the extent this claim can be amended consistent with this Order.

3 7. Count VII – Negligence.

4 The elements of a claim for negligence under California law are: “(1) a legal duty to
5 use due care; (2) a breach of such legal duty; and (3) the breach as the proximate or legal cause of the
6 resulting injury.” 6 Witkin, Summary of Cal. Law, Torts § 835, p. 52 (10th ed. 2005). In this
7 context, “legal duty” means the duty to use ordinary care in activities from which harm to the
8 plaintiff might reasonably be anticipated. *See id.* at p. 53. ““The risk reasonably to be perceived
9 defines the duty to be obeyed.”” *Dillon v. Legg*, 68 Cal.2d 728, 739 (Cal. 1968) (quoting *Palsgraf v.*
10 *Long Island R.R. Co.* 248 N.Y. 339, 344 (N.Y. 1928)).

11 According to the FAC, “Defendant owed a duty to Plaintiff and Class Members to protect
12 their personal information and data property and take reasonable steps to protect them from the
13 wrongful taking of such information and the wrongful invasion of their privacy.” (FAC ¶ 205.)
14 Defendant allegedly breached this duty by, among other things, accessing and uploading data from
15 Plaintiff’s Contact Address Book, storing that data in an unsecure manner, and transmitting the data
16 to third parties. (*Id.* ¶ 208; *see also, id.* ¶ 203 (incorporating by reference paragraphs 1 through
17 202).) Plaintiff complains of two injuries: (a) diminished bandwidth; and (b) the cost of removing
18 tracking software. (*See id.* ¶ 209 (citing *id.* ¶¶ 56-79, 108-11, and 121-23).)

19 Defendant argues that Plaintiff has not provided any legal basis for the alleged duty. The
20 case on which Defendant relies, *In re iPhone Application Litig.*, 2011 WL 4403963 (N.D. Cal.
21 2011), does not support its position. There, Judge Koh found that the “Plaintiffs ha[d] not yet
22 adequately pled or identified a legal duty on the part of Apple to protect users’ personal information
23 from third-party app developers.” *Id.* at *9. No such duty to protect Plaintiff from third parties is
24 alleged here – Path *is* a third-party app developer and Plaintiff alleges that Path had a duty not to
25 take Plaintiff’s personal information. Path has not offered any legal authority to support its position
26 that it does not owe Plaintiff such a duty. Based upon the facts alleged in the FAC, and the
27 arguments advanced by Path, the Court cannot rule as a matter of law that Path did not owe Plaintiff
28

1 a duty not to take his personal information. *See Rowland v. Christian*, 69 Cal.2d 108, 112 (Cal.
2 1968) (absent statutory provision or public policy declaring exception to fundamental principle that
3 a person is liable for injuries caused by failure to exercise reasonable care, no such exception should
4 be made).

5 Path also argues, on the same grounds that it argued Plaintiff does not have standing, that
6 Plaintiff has not alleged an appreciable, non-speculative, present injury. The Court already
7 addressed this issue in its Standing analysis, *supra*, Part II, and found that the cost of removing
8 tracking software sufficiently alleges injury-in-fact for purposes of withstanding a motion to dismiss.

9 Based on the foregoing analysis, the Court **DENIES** the Motion to Dismiss Count VII.

10 8. Count VIII – Conversion.

11 The tort of conversion requires that a plaintiff plead “ownership or right to possession
12 of property, wrongful disposition of the property right and damages.” *Kremen v. Cohen*, 337 F.3d
13 1024, 1029 (9th Cir. 2003) (quoting *G.S. Rasmussen & Assocs., Inc. v. Kalitta Flying Serv., Inc.*, 958
14 F.2d 896, 906 (9th Cir. 1992).

15 Path argues that it has not dispossessed or excluded Plaintiff from use of that property
16 because Plaintiff has only alleged that Path copied the information. Plaintiff does not dispute that he
17 does not allege the second element for a claim of conversion, wrongful disposition of the property
18 right, which the Court takes as a tacit concession of the merits of Path’s argument. Accordingly, the
19 Court will dismiss the claim on this ground.

20 Based on the foregoing analysis, the Court **GRANTS** the Motion to Dismiss Count VIII. Out of
21 an abundance of caution that the element of wrongful disposition of a property right can, in fact, be
22 alleged specifically, the Court grants **LEAVE TO AMEND** to the extent this claim can be amended
23 consistent with this Order.

24 9. Count IX – Trespass.

25 The tort of trespass to chattels has been extended to cases where the plaintiff can
26 establish that “(1) defendant intentionally and without authorization interfered with plaintiff’s
27 possessory interest in [a] computer system; and (2) defendant’s unauthorized use proximately
28 resulted in damage to plaintiff.” *eBay, Inc. v. Bidder’s Edge, Inc.*, 100 F. Supp. 2d 1058, 1069-1070

1 (N.D. Cal. 2000). The California Supreme Court has held that the tort “does not encompass ... an
2 electronic communication that neither damages the recipient computer system nor impairs its
3 functioning.” *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1347 (Cal. 2003); *see also id.* at 1356 (“In the
4 decisions so far reviewed, the defendant’s use of the plaintiff’s computer system was held sufficient
5 to support an action for trespass when it actually did, or threatened to, interfere with the intended
6 functioning of the system, as by significantly reducing its available memory and processing power.”).

7 As to the first element, Plaintiff adequately pleads that the alleged interference was
8 unauthorized because, although he downloaded the Path App, Path exceeded the scope of any
9 consent given. More problematic is that Plaintiff has not alleged that the functioning of his mobile
10 device was *significantly* impaired to the degree that would enable him to plead the elements of a
11 trespass—as alleged in the FAC, any depletion of his mobile device’s finite resources is a *de minimis*
12 injury.

13 Based on the foregoing analysis, the Court **GRANTS** the Motion to Dismiss Count IX. Out of
14 an abundance of caution that Plaintiff can allege more than a *de minimus* injury, the Court grants
15 **LEAVE TO AMEND** to the extent this claim can be amended consistent with this Order.

16 *10. Count X – Unjust Enrichment.*

17 Path moves for dismissal of Count X on the basis that unjust enrichment is not a cause
18 of action under California law. California Courts are split on this issue. *See Hill v. Roll Int’l Corp.*,
19 195 Cal. App. 4th 1295, 1307 (Cal. Ct. App. 2011); *In re iPhone Application Litig.*, *supra*, 2011 WL
20 4403963, at *15. Depending on the nature of the allegations, a cause of action for unjust enrichment
21 could exist. *See* RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT § 1 (2012). This
22 Court previously held that there is a cause of action for unjust enrichment under California law. *See,*
23 *e.g., Hawthorne v. Umpqua Bank*, C-11-6700 YGR, Dkt. No. 30, 2012 WL 1458194, at *2-3 (N.D.
24 Cal. Apr. 26, 2012). Therefore, the Court denies the motion on this basis.

25 Based on the foregoing, the Court **DENIES** the Motion to Dismiss Count X for Unjust
26 Enrichment.

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

IV. CONCLUSION

For the reasons set forth above, the Motion to Dismiss is **GRANTED IN PART WITH LEAVE TO AMEND**. Counts I, II, IV, VI, VIII, and IX are **DISMISSED WITH LEAVE TO AMEND**.

By no later than November 9, 2012, Plaintiff shall file either a second amended complaint or a statement that he will proceed on the first amended complaint.

Defendant shall respond within 21 days of service.

This Order Terminates Docket Number 16.

IT IS SO ORDERED.

Dated: October 17, 2012



YVONNE GONZALEZ ROGERS
UNITED STATES DISTRICT COURT JUDGE