

1  
2  
3  
4  
5  
6  
7 MARC OPPERMAN, et al.,  
8 Plaintiffs,  
9 v.  
10 PATH, INC., et al.,  
11 Defendants.

Case No. 13-cv-00453-JST

**ORDER DENYING YELP'S MOTION  
FOR SUMMARY JUDGMENT**

Re: Dkt. No. 689

12 Before the Court is Defendant Yelp, Inc.'s motion for summary judgment. The Court will  
13 deny the motion.

14 **I. BACKGROUND**

15 Plaintiffs challenge conduct by Apple and various developers of applications ("apps") for  
16 Apple devices. See Second Consolidated Amended Complaint ("SCAC"), ECF No. 478.  
17 Plaintiffs allege that Yelp and other app developers improperly uploaded address book data from  
18 their phones without their consent. See, e.g., id. ¶¶ 119-120. Yelp now moves for summary  
19 judgment on the ground that Plaintiffs consented to allow this uploading.

20 **A. Contacts Data**

21 The facts of this putative class action have been recited in detail in prior orders and require  
22 only a brief summary here. Each Apple device comes pre-loaded with a "Contacts" app that  
23 owners may use as an address book to input and store various information about the owner's  
24 contacts. Id. ¶ 54, 55. The Plaintiffs allege that this information "is highly personal and private,  
25 and "is not shared, is not publicly available, is not publicly accessible, and is not ordinarily  
26 obtainable by a third party unless the owner physically relinquishes custody of his or her device to  
27 another individual." Id. ¶ 56. Plaintiffs further allege that Yelp and other app developers  
28 uploaded their contacts data without their consent.

1           **B.       The Yelp App’s “Friend Finder” Feature**

2           The Yelp app introduced a Friend Finder” feature on approximately January 16, 2010.<sup>1</sup>  
3 ECF No. 689-1 ¶ 4. This feature allowed Yelp users to locate other Yelp users they know by  
4 comparing the email addresses in the user’s local Contacts app with a database of email addresses  
5 of registered Yelp users. Id. ¶ 2.

6           Yelp’s “Friend Finder” feature was only available to registered Yelp users who agreed to  
7 Yelp’s Terms of Service and Privacy Policy. Id. ¶¶ 2, 3. To create a Yelp account, a user must  
8 complete the online registration process by accessing Yelp’s website on a computer or through the  
9 mobile app. Id. Before a user can advance past the first page of the registration process, he or she  
10 must click on a red button. Id. ¶ 3. The following statement appears above the red button: “By  
11 clicking the button below, you agree to Yelp’s Terms of Service and Privacy Policy.”<sup>2</sup> Id. In turn,  
12 if one clicks on the blue hyperlinked text reading “Terms of Service” or “Privacy Policy,” he or  
13 she is taken to a web page that displays those policies. Id. The Yelp Privacy Policy in effect on

---

15           <sup>1</sup> The Plaintiffs contend that the declaration of Yelp’s engineer, Steven Sheldon, is inadmissible.  
16 ECF No. 727 at 9. Specifically, they argue that the declaration is inadmissible because  
17 (1) Sheldon was not disclosed as a witness in Yelp’s initial disclosures, and (2) Sheldon was hired  
18 after the class period and therefore lacks personal knowledge. Id. In response, Yelp argues that it  
intends to use Mr. Sheldon as an expert witness; expert witness identifications are not due until  
January 2017; and the failure to disclose him as a witness in their initial disclosures was harmless.  
ECF No. 759 at 6.

20           A party that “fails to provide information or identify a witness as required by Rule 26(a) or (e) . . .  
21 is not allowed to use that information or witness to supply evidence on a motion, at a hearing, or at  
22 a trial, unless the failure was substantially justified or is harmless.” Fed. R. Civ. P. 37(c)(1).  
Under Rule 26(a)(2), Yelp is required to disclose its expert witnesses “at the time and in the  
23 sequence that the court orders.” Fed. R. Civ. P. 26(a)(2)(D). Here, the Court ordered the parties  
to identify their expert witnesses by January 2017. ECF No. 712. Therefore, Yelp has not failed  
24 to timely identify Sheldon as an expert witness as required by Rule 26(a), and his declaration is  
not rendered inadmissible by Rule 37(c)(1). The Court also concludes that Sheldon may provide  
expert testimony based on his knowledge and examination of Yelp’s source code as one of Yelp’s  
25 engineers regardless of whether he was employed at Yelp during the class period. See Fed. R.  
Evid. 703; see also *Cree v. Flores*, 157 F.3d 762, 773 (9th Cir. 1998) (“Mr. Yallup testified as an  
26 expert witness; therefore, his testimony was not subject to the strictures of Federal Rules of  
Evidence 602 [requiring personal knowledge] and 803.”).

27           <sup>2</sup> Although the exact language of this statement has changed slightly over the years, it has  
28 remained substantially the same since at least September 15, 2008. Id.

1 September 21, 2011 stated, in part:

2 Contacts: You can invite your friends to join the Site by providing their contact  
3 information or by allowing us to use your address book from your computer,  
4 mobile device, or other sites. If you invite a friend to join and connect with you on  
5 the Site, we may use and store your friends' contact information long enough to  
process your requests.

6 Request for Judicial Notice in Support of Yelp's Motion for Summary Judgment, ECF No. 690,  
7 Ex. B at 2.<sup>3</sup> The Yelp Privacy Policy in effect on May 26, 2009 included the following notice  
8 about contacts data:

9 You may choose to provide us with another person's e-mail address so that person  
10 may be invited to create an account on this website and become your friend. We  
11 use this information to contact and, if necessary, remind that person about the  
12 invitation. By providing us with another person's e-mail address, you represent to  
13 us that you have obtained the consent of the person concerned as regards such  
14 disclosure to us of their personal information. All invitees are provided with the  
15 option not to receive further invitations.

16 Id., Ex. A at 4. Once the user created a Yelp account and agreed to the Terms of Service and  
17 Privacy Policy, he or she would be able to access the "Friend Finder" feature in the Yelp app on  
18 their mobile device. ECF No. 689-1 ¶ 4.

19 A registered Yelp user who navigated to the "Friend Finder" feature between January 16,  
20 2010 and February 22, 2012 would see the following pop-up dialog box:

21  
22  
23  
24 <sup>3</sup> The Court takes judicial notice of the Yelp Privacy Policies during the relevant time periods  
25 because they were publicly available on the Yelp website and their existence cannot reasonably be  
26 questioned. See Fed. R. Evid. 201; see also, e.g., Datel Holdings, Ltd. v. Microsoft Corp., 712 F.  
27 Supp. 2d 974, 983–84 (N.D. Cal. 2010) (taking judicial notice of an Xbox software license and  
28 terms of use that were available online and noting that these documents were "judicially noticeable  
for the fact that they exist, not whether, for example, the documents are valid or binding  
contracts").



Id.<sup>4</sup> Between February 22, 2012 and March 8, 2012, the dialog box was changed to read the following: “Find Friends. We’ll need to look at your contacts to find friends. Don’t worry, we’re not storing them.” Id. Underneath that dialog box, the user could select either “No Thanks” or “OK.” Id. During either time period, if the user clicked “Yes, Find Friends” or “OK” the Yelp app transmitted the email addresses in the user’s Contacts app to Yelp’s servers and cross-checked those email addresses against the email addresses of registered Yelp users. Id. ¶ 5.

### C. Apple’s Review of the Yelp App

As an app developer, Yelp was bound by several contracts with Apple. Yelp entered into a Program License Agreement (“PLA”) in which it appointed Apple as its “worldwide agent for the delivery of [its app].” ECF No. 727-6, Ex. C at 2, 7-8, § 3.1(e). The PLA provides that “applications may not collect user or device data without prior user consent.” Id. at 9, § 3.3.9. Yelp was also subject to Apple’s App Store Review Guidelines. ECF No. 727-5, Ex. B at 3, § 1.1. Guideline 17.1 provides that “[a]pps 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.” Id. at 16, § 17.1.

---

<sup>4</sup> For a short period of time between January 2010 and March 2010, the text was slightly different: The prompt read “Find friends using your Contacts and Facebook friends? You’ll be able to see their bookmarks and find out when they are nearby.” Id. This minor change in verbiage does not affect the Court’s analysis.

1       In February 2012, Apple conducted an internal technical investigation to determine  
2 whether certain apps, including Yelp, complied with its privacy guidelines. Apple concluded that  
3 the “[o]ld version sends contact data up to yelp.com without the user’s permission.” ECF No 727-  
4 7, Ex. D at16. Even though Yelp had recently changed the dialog box to alert users that the app  
5 would “need to look at your contacts to find friends,” Apple nonetheless concluded that the “[n]ew  
6 version . . . doesn’t inform the user that the date [sic] is uploaded to yelp.com.” Id. at 16, 18, 20  
7 (“The alert should clarify to the user that their data is being uploaded to yelp.com.”).

8       In response to this internal investigation, Yelp changed its pop up dialog box to display the  
9 following message: “To find friends, *we’ll need to upload your contacts to Yelp*. Don’t worry,  
10 we’re not storing them.” ECF No. 689-1 ¶ 4 (emphasis added); ECF No. 727-7, Ex. D at 2; ECF  
11 No. 727-4, Ex. A at 3. The Plaintiffs do not challenge Yelp’s conduct after these changes were  
12 implemented. ECF No. 727 at 16:2.

13           **D. Public Response**

14       Around the same time Apple was conducting its internal investigation, major media  
15 sources began reporting about the alleged privacy breach. See Plaintiff’s Request for Judicial  
16 Notice, ECF No. 749, Exs. A-F; Plaintiff’s Request for Judicial Notice, ECF No. 728, Exs. A-F.<sup>5</sup>  
17 Congress reacted by opening an inquiry into Apple’s privacy practices. See ECF No. 748-11, Ex.  
18 J; ECF No. 748-12, Ex. K; see also Protecting Mobile Privacy: Your Smartphones, Tablets, Cell  
19 Phones and Your Privacy: Hearing Before the Subcommittee on Privacy, Tech. and the Law of the  
20 S. Judiciary Comm., 112th Cong. (2011), available at

21  
22 \_\_\_\_\_  
23       <sup>5</sup> The Plaintiffs ask the Court to take judicial notice of several news articles from sources including  
24 the New York Times, Time Magazine, and the British Broadcasting Corporation. See ECF No.  
25 749 at 2; ECF No. 728 at 2. Pursuant to Federal Rule of Evidence 201(b), “[t]he court may  
26 judicially notice a fact that is not subject to reasonable dispute because it: (1) is generally known  
27 within the trial court’s territorial jurisdiction; or (2) can be accurately and readily determined from  
28 sources whose accuracy cannot reasonably be questioned.” The Court “may take judicial notice of  
publications introduced to indicate what was in the public realm at the time, not whether the  
contents of those articles were in fact true.” Von Saher v. Norton Simon Museum of Art at  
Pasadena, 592 F.3d 954, 960 (9th Cir. 2009) (internal quotation marks omitted). The Court  
therefore takes judicial notice of these publications “solely as an indication of what information  
was in the public realm at the time.” Von Saher, 592 F.3d at 960.

1 https://www.judiciary.senate.gov/imo/media/doc/CHRG-112shrg86775.pdf. And the Federal  
2 Trade Commission also issued a Civil Investigative Demand to investigate whether apps uploaded  
3 user's contacts without their consent. See ECF No. 748-13, Ex. L.

4 **E. Procedural History**

5 Plaintiffs brought this suit against Apple and several app developers, including Yelp, as a  
6 putative class action.<sup>6</sup> See ECF Nos. 362, 478. The Plaintiffs allege that Yelp uploaded address  
7 book data from their Contacts app without their consent. See SCAC, ECF No. 478, ¶¶ 2, 119, 120,  
8 146, 178, 184, 195, 208. Based on these allegations, the Plaintiffs assert a cause of action for  
9 invasion of privacy (intrusion upon seclusion) against Yelp. See id. ¶¶ 243-255 (alleging that  
10 Yelp and the other App defendants "intentionally intruded on and into each respective Plaintiff's  
11 solitude, seclusion or private affairs" by "surreptitiously obtaining, improperly gaining knowledge,  
12 reviewing and retaining Plaintiffs' private address books (or substantial portions thereof) as stored  
13 in the Contacts App on Plaintiffs' iDevices"). This is the only remaining claim against Yelp. See  
14 ECF Nos. 471, 543 (dismissing all other claims).

15 **II. JURISDICTION**

16 The Court has subject matter jurisdiction over this action under the Class Action Fairness  
17 Act of 2005. The amount in controversy exceeds the sum or value of \$5,000,000, exclusive of  
18 interests and costs; there are 100 or more class members; and there is minimal diversity because  
19 certain members of the class are citizens of a different state than any Defendant as required by 28  
20 U.S.C. § 1332(d)(2).

21 **III. LEGAL STANDARD**

22 Summary judgment is proper when a "movant shows that there is no genuine dispute as to  
23 any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a).  
24 "A party asserting that a fact cannot be or is genuinely disputed must support the assertion by"  
25 citing to depositions, documents, affidavits, or other materials. Fed. R. Civ. P. 56(c)(1)(A). A

---

26  
27 <sup>6</sup> The Court recently certified a limited class against another app developer defendant, Path, Inc.,  
28 based on allegations similar to those against Yelp. ECF No. 761 at 28.

1 party may also show that such materials “do not establish the absence or presence of a genuine  
2 dispute, or that an adverse party cannot produce admissible evidence to support the fact.” Fed. R.  
3 Civ. P. 56(c)(1)(B). An issue is “genuine” only if there is sufficient evidence for a reasonable  
4 fact-finder to find for the non-moving party. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248–  
5 49 (1986). A fact is “material” if the fact may affect the outcome of the case. Id. at 248. “In  
6 considering a motion for summary judgment, the court may not weigh the evidence or make  
7 credibility determinations, and is required to draw all inferences in a light most favorable to the  
8 non-moving party.” Freeman v. Arpaio, 125 F.3d 732, 735 (9th Cir. 1997).

9 Where the party moving for summary judgment would bear the burden of proof at trial,  
10 that party bears the initial burden of producing evidence that would entitle it to a directed verdict if  
11 uncontested at trial. See C.A.R. Transp. Brokerage Co. v. Darden Rests., Inc., 213 F.3d 474,  
12 480 (9th Cir. 2000). Where the party moving for summary judgment would not bear the burden of  
13 proof at trial, that party bears the initial burden of either producing evidence that negates an  
14 essential element of the non-moving party’s claim, or showing that the non-moving party does not  
15 have enough evidence of an essential element to carry its ultimate burden of persuasion at trial.

16 If the moving party satisfies its initial burden of production, then the non-moving party  
17 must produce admissible evidence to show that a genuine issue of material fact exists. See Nissan  
18 Fire & Marine Ins. Co. v. Fritz Cos., 210 F.3d 1099, 1102–03 (9th Cir. 2000). The non-moving  
19 party must “identify with reasonable particularity the evidence that precludes summary judgment.”  
20 Keenan v. Allan, 91 F.3d 1275, 1279 (9th Cir. 1996). Indeed, it is not the duty of the district court  
21 to “to scour the record in search of a genuine issue of triable fact.” Id. “A mere scintilla of  
22 evidence will not be sufficient to defeat a properly supported motion for summary judgment;  
23 rather, the nonmoving party must introduce some significant probative evidence tending to support  
24 the complaint.” Summers v. Teichert & Son, Inc., 127 F.3d 1150, 1152 (9th Cir. 1997) (citation  
25 and internal quotation marks omitted). If the non-moving party fails to make this showing, the  
26 moving party is entitled to summary judgment. Celotex Corp. v. Catrett, 477 U.S. 317, 323  
27 (1986).

**IV. DISCUSSION**

Under California law,<sup>7</sup> a claim for intrusion upon seclusion has two elements: (1) intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person. Shulman v. Grp. W Prods., Inc., 18 Cal. 4th 200, 231 (1998), as modified on denial of reh'g (July 29, 1998); see also Restatement (Second) of Torts § 652B (1977) (“One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person”). The Court now addresses whether the Plaintiffs have produced evidence of these elements such that they could carry their burden at trial.

**A. Consent**

Yelp argues that the Plaintiffs’ intrusion upon seclusion claim fails as a matter of law because the Plaintiffs consented to allow Yelp to access their local Contacts app to find friends, thereby defeating any reasonable expectation of privacy in their address book data and any potential intrusion upon seclusion claim. See ECF No. 689 at 18-19.

Effective consent negates an intrusion upon seclusion claim. See Restatement (Second) of Torts § 892A (1979) (“One who effectively consents to conduct of another intended to invade his interests cannot recover in an action of tort for the conduct or for harm resulting from it.”). To satisfy the first element of an intrusion upon seclusion claim, the plaintiff must have had “an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source.” Shulman, 18 Cal. 4th at 232; see also Varnado v. Midland Funding LLC, 43 F. Supp. 3d 985, 992 (N.D. Cal. 2014). And a plaintiff cannot have a reasonable expectation of privacy if she consented to the intrusion. Hill v. Nat'l Collegiate Athletic Assn., 7 Cal. 4th 1, 26, 865 P.2d 633 (1994) (“The plaintiff in an invasion of privacy case must have conducted himself or herself in a manner consistent with an actual expectation of privacy, i.e., he or she must not have manifested

---

<sup>7</sup> Although the laws of several states are potentially implicated because the Plaintiffs reside in different states, Yelp concedes that “for the purposes of this motion, the [state law] standards are congruent.” ECF No. 689 at 15, n. 2. Accordingly, the Court applies California law.

1 by his or her conduct a voluntary consent to the invasive actions of defendant.”). Therefore, if the  
2 Plaintiffs effectively consented to Yelp’s use of their address book data, they cannot maintain an  
3 intrusion upon seclusion claim. In addition, “[i]f voluntary consent is present, a defendant’s  
4 conduct will rarely be deemed ‘highly offensive to a reasonable person’ so as to justify tort  
5 liability.” Hill, 7 Cal. 4th at 26.

6 However, consent is only effective if the person alleging harm consented “to the particular  
7 conduct, or to substantially the same conduct” and if the alleged tortfeasor did not exceed the  
8 scope of that consent. Restatement (Second) of Torts § 892A (1979) §§ 2(b), 4. After all,  
9 “privacy, for purposes of the intrusion tort, is not a binary, all-or-nothing characteristic.” Sanders  
10 v. Am. Broad. Companies, Inc., 20 Cal. 4th 907, 916 (1999). “There are degrees and nuances to  
11 societal recognition of our expectations of privacy: the fact that the privacy one expects in a given  
12 setting is not complete or absolute does not render the expectation unreasonable as a matter of  
13 law.” Id.

14 Yelp argues that the Plaintiffs “allowed . . . Yelp’s access to their Contacts list to perform  
15 the precise function they desired: to connect with their friends to improve the Apps’ social  
16 networking experiences.” ECF No. 689 at 19. In response, the Plaintiffs argue that consent to  
17 “access” or “look at” their contacts is not the same as consent to “upload” those contacts. ECF  
18 No. 727 at 23. In other words, “permission to look at data does not equate with permission to take  
19 it.” Id. at 7. At the summary judgment stage, the Court agrees with the Plaintiffs.

20 There is a material factual dispute as to whether Yelp’s in-app user prompt obtained  
21 effective consent to *upload* the address book data to its servers. The Plaintiffs point to several  
22 pieces of evidence that a reasonable fact-finder could rely on to find in their favor. First, the  
23 textual in-app display did not explicitly disclose that Yelp would “upload” the address book data  
24 to its own servers in order to perform the matching function. Rather, the text of the disclosure  
25 during the class period simply told users that the feature would “[f]ind friends on Yelp using your  
26 Contacts” or “look at your contacts to find friends.” ECF No. 689-1 ¶ 4. And the Plaintiffs have  
27 produced evidence suggesting that, based on these disclosures, they expected a matching process  
28 that would take place locally on their phone, not on Yelp’s servers. See Depo. Tr. of Claire

1       Hodgins, ECF No. 759-3 at 10-22 (testifying that she thought the matching process would take  
2 place “on [her] phone”). Second, Yelp’s own agent (Apple) concluded that both versions of  
3 Yelp’s disclosure during the class period “send[] contact data up to yelp.com without the user’s  
4 permission” and “[don’t] inform the user that the date [sic] is uploaded to yelp.com.” ECF No  
5 727-7, Ex. D at 16, 18, 20. Apple’s privacy guidelines suggest that app users had a reasonable  
6 expectation of privacy in knowing how their data would be used, and the breach of those  
7 guidelines suggests that Yelp exceeded the scope of users’ consent when it uploaded Contacts data  
8 without explicit permission. See Puerto v. Superior Court, 158 Cal. App. 4th 1242, 1252 (2008)  
9 (holding that employees had a legitimate expectation of privacy in their addresses and telephone  
10 numbers “in light of employers’ usual confidentiality customs and practices”). Based on this  
11 evidence, the Court cannot conclude as a matter of law that the in-app disclosures obtained  
12 effective consent to upload the users’ Contacts data as opposed to just accessing it locally. This is  
13 an issue for the jury.

14       Nor can the Court conclude as a matter of law that Yelp’s additional layer of disclosure—  
15 its Terms of Service and Privacy Policy—obtained effective consent to upload users’ contacts data  
16 to its servers. Yelp argues that “each Plaintiff consented to that access not once but *at least* twice,  
17 first when registering as a Yelp user and agreeing to be bound by the Terms of Service and  
18 Privacy Policy, and again when using the Friend Finder function.” ECF No. 689 at 19:13-15.  
19 There are two problems with Yelp’s reliance on its Privacy Policy, however. First, it is unclear  
20 whether the hyperlinked, off-screen terms in the Privacy Policies provided users with constructive  
21 notice such that they could effectively consent to anything contained off-screen. In fact, Ninth  
22 Circuit precedent suggests otherwise:

23       [W]here a website makes its terms of use available via a conspicuous hyperlink on every  
24 page of the website but otherwise provides no notice to users nor prompts them to take any  
25 affirmative action to demonstrate assent, even close proximity of the hyperlink to relevant  
26 buttons users must click on—without more—is insufficient to give rise to constructive  
27 notice. While failure to read a contract before agreeing to its terms does not relieve a party  
28 of its obligations under the contract, the onus must be on website owners to put users on  
notice of the terms to which they wish to bind consumers.

Nguyen v. Barnes & Noble Inc., 763 F.3d 1171, 1178–79 (9th Cir. 2014) (internal citations

omitted). Second, even assuming that the Privacy Policy provided constructive notice to users of the terms by which they would be bound, a reasonable jury could find that Yelp’s Privacy Policy provisions do not explicitly address—and thus do not obtain knowing consent for—the uploading of a user’s address book data for the purpose of finding friends who are already registered Yelp users. The Privacy Policy provisions cited by Yelp only speak to how Yelp will use a user’s friend’s contact information when they “invite . . . friends to join the Site” or “provide [Yelp] with another person’s e-mail address so that person may be invited to create an account on this website.” ECF No. 690, Ex. B at 2; ECF No. 690, Ex. A at 4. In that situation, the Privacy Policy explains, Yelp “may use and store your friends’ contact information long enough to process your requests” and the user “represent[s] to [Yelp] that [he or she] has obtained the consent of the person concerned.” Id. But that is not the situation that the Plaintiffs are complaining about in this lawsuit. The “Friend Finder” function at issue here did not obtain the email addresses from a user’s Contacts to invite friends to create an account on Yelp; rather, it obtained the email addresses from a user’s Contacts to cross-check those email addresses against *already-registered Yelp users*. In sum, it is unclear whether the language in the relevant Privacy Policy provisions even applies to the Friend Finder function at issue in this lawsuit. Given this ambiguity, the Court cannot conclude as a matter of law that these Privacy Policy provisions obtained effective consent to upload a user’s friend’s email address from their Contacts app for the purpose of finding friends that already had Yelp accounts.

Throughout its briefing, Yelp argues that the Plaintiffs’ intrusion upon seclusion claim only survived the prior motions to dismiss because the Plaintiffs alleged that Yelp “misused” or “misappropriated” the address book data in other, unauthorized ways – such as storing, disseminating, or selling the data. ECF No. 689 at 7-8, 13; ECF No. 759 at 14, 17. Accordingly, Yelp argues that, because the Plaintiffs have not produced evidence of these *particular* kinds of unauthorized use their claim fails as a matter of law. Id.

Yelp reads the Court’s previous orders and the crux of the Plaintiffs’ allegations too narrowly. The Court has not said, and the Plaintiffs have not alleged, that these are the only ways that Yelp could have overstepped the bounds of the consent it obtained. Rather, the Plaintiffs also

1 alleged, and the Court found plausible when ruling on multiple motions to dismiss, that  
2 “Defendants had exceeded the parameters of that consent by otherwise transmitting, *uploading*,  
3 storing, and using that information for unauthorized purposes or in unauthorized ways.” ECF No.  
4 543 at 32 (emphasis added). Although the Court noted that discovery might ultimately prove that  
5 allegation to be unfounded, the Court reached no ultimate conclusion on the issue. Id. at 33, n. 17.  
6 (“After further factual development, Defendants may succeed in demonstrating that the parameters  
7 of Plaintiffs’ consent was coterminous with Defendants’ use of that data. But that is a matter that  
8 cannot be resolved at this stage of the proceedings.”). That discovery having now taken place, it is  
9 clear that the issue cannot be decided as a matter of law.

10       Yelp relies on two cases to further support its consent argument: Hill v. Nat'l Collegiate  
11 Athletic Assn., 7 Cal. 4th 1, 26 (1994) and Perkins v. LinkedIn Corp., 53 F. Supp. 3d 1190 (N.D.  
12 Cal. 2014). ECF No. 689 at 18. Both cases are distinguishable.

13       In Hill, student athletes brought invasion of privacy claims against the NCAA under the  
14 California Constitution based on the NCAA’s requirement that student athletes undergo drug  
15 testing. The California Supreme Court held that the athletes manifested voluntary consent to the  
16 testing, thereby defeating their invasion of privacy claim. See Hill, 7 Cal. 4th at 42. However, the  
17 plaintiffs in that case were “required to sign a three-part statement and consent form,” which  
18 included the following “Drug-Testing Consent” provision: “By signing this part of the form, you  
19 certify that you agree to be tested for drugs.” Id. at 11. Based on this explicit consent form, the  
20 Court held that the student athletes had a diminished expectation of privacy. Id. at 42. Here,  
21 unlike in Hill, Yelp’s brief screen prompt did not explicitly disclose that it would upload users’  
22 address book data. Hill does not dispose of the present case.

23       Perkins is also distinguishable. In that case, the court held that LinkedIn remained within  
24 the scope of the consent that it obtained from users when it sent an email inviting their contacts to  
25 join LinkedIn, but that it exceeded the scope of that consent when it sent subsequent reminder  
26 emails. Id. at 1215-17. LinkedIn’s disclosures said “Why not invite some people?” and “Stay in  
27 touch with your contacts who aren’t on LinkedIn yet. Invite them to connect with you.” Id. at  
28 1215. If a user agreed to invite people, LinkedIn sent an email to the contact that said “I’d like to

1 add you to my professional network” with the name of the LinkedIn user below. Id. The  
2 plaintiffs conceded that they consented to LinkedIn sending an email to their contacts to invite  
3 them to connect on LinkedIn; however, they argued that they did *not* consent to an email in which  
4 their own name would be displayed as a personal “endorsement” of LinkedIn. Id. The court was  
5 not persuaded by the plaintiffs’ distinction between “invitations” and “endorsements,” and  
6 concluded that those terms were “synonymous” in that instance. Id. The users agreed to a  
7 disclosure that said “Invite [contacts] to connect with *you*,” and “a reasonable user who saw the  
8 disclosure” consented to an email that necessarily included his or her own name for the purpose of  
9 fostering a connection. Id. (emphasis added). In other words, LinkedIn obtained consent to invite  
10 a user’s friends to connect with him or her, which necessarily involved mentioning the other user  
11 by name. In contrast to Perkins, it is unclear whether a reasonable user who saw Yelp’s disclosure  
12 message consented to having the email addresses in their local Contacts uploaded to a Yelp server  
13 in order to perform the matching function. The disclosure simply said “[f]ind friends on Yelp  
14 using your Contacts” or “*look at* your contacts to find friends.” ECF No. 689-1 ¶ 4 (emphasis  
15 added). Unlike in Perkins, where consent to the disclosure message necessarily included consent  
16 to put the user’s name in the invitation email, consent to allow Yelp to “find friends” or “look at”  
17 the contacts on your device does not necessarily include consent to upload that data to Yelp’s  
18 servers; rather, a reasonable user could think that the matching function would take place on their  
19 local device. In other words, “upload” and “look at” are not interchangeable.

20 In fact, Yelp’s argument ignores Perkins’ implicit holding that consent is defined by the  
21 scope of its terms. Yelp argues that “[o]nce Plaintiffs consented to Yelp’s access to that  
22 information, the alleged tort evaporates; there is no invasion to begin with, and subsequent  
23 transmission cannot change that.” ECF No. 689 at 13:9-10. In contrast, the California Supreme  
24 Court has said that “privacy, for purposes of the intrusion tort, is not a binary, all-or-nothing  
25 characteristic.” Sanders, 20 Cal. 4th at 916. Rather, “[t]here are degrees and nuances to societal  
26 recognition of our expectations of privacy,” and “the fact that the privacy one expects in a given  
27 setting is not complete or absolute does not render the expectation unreasonable as a matter of  
28 law.” Id.; see also e.g., Sheehan v. San Francisco 49ers, Ltd., 45 Cal. 4th 992 (2009) (“Hill does

1 not stand for the proposition that a person who chooses to attend an entertainment event consents  
2 to *any* security measures the promoters may choose to impose no matter how intrusive or  
3 unnecessary. . . . a person can be deemed to consent only to intrusions that are reasonable under  
4 the circumstances.”). Like the California Supreme Court in Sanders, the court in Perkins made  
5 clear that users can consent to some aspects of a defendant’s conduct while not consenting to other  
6 aspects of a defendant’s conduct. For example, the court in Perkins held that, although the  
7 plaintiffs consented to LinkedIn’s initial endorsement email, they had “plausibly alleged that they  
8 did not consent to the second and third reminder endorsement emails.” 53 F. Supp. 3d at 1216.  
9 Because “[n]othing in LinkedIn’s disclosures alerts users to the possibility that their contacts will  
10 receive not just one invitation, but three,” the court held that “Plaintiffs have adequately pleaded  
11 lack of consent to the sending of the second and third endorsement emails.” Id. at 1217. In sum,  
12 Perkins reaffirms that consent is not absolute, but rather a matter of degree. And, like the court in  
13 Perkins, a reasonable jury could find that nothing in Yelp’s disclosures alerted users to the  
14 possibility that their contacts’ email addresses would be uploaded to Yelp’s servers in order to  
15 perform the matching function.

16 In response, Yelp argues that “the operation of the Friend Finder function . . . inevitably  
17 requires that data be transmitted from the users’ phone to Yelp’s servers for processing.” ECF No.  
18 759 at 14:8-10. This statement misses the point. The question is not whether Yelp’s engineers  
19 establish during litigation that the only feasible way to compare the users’ contacts to registered  
20 Yelp users is to upload the contacts to Yelp’s server. The question is whether, and to what extent,  
21 the Plaintiffs effectively consented to allow Yelp to use their contact data at the time of the  
22 challenged invasion.<sup>8</sup> Cf. Hill, 7 Cal. 4th at 26 (“The plaintiff in an invasion of privacy case must  
23 have conducted himself or herself in a manner consistent with an actual expectation of privacy,

24  
25 \_\_\_\_\_  
26 <sup>8</sup> Yelp mentions throughout its Reply brief that “all of the Plaintiffs now know that the Apps at  
27 issue (and others) have to upload data to analyze it, and yet all of them continue to consent to  
multiple applications using their Contacts.” ECF No. 759 at 15:5-7; id. at 13:6-8. The Plaintiffs’  
28 current knowledge that Yelp uploads their address book data is irrelevant to whether they  
effectively consented to Yelp’s uploading of their data at the time of the challenged conduct.

1 i.e., he or she must not have manifested by his or her conduct a voluntary consent to the invasive  
2 actions of defendant.”). This inquiry hinges on the “objectively reasonable expectation[s]” of the  
3 Plaintiffs. Shulman, 18 Cal. 4th at 232.

4 Perhaps recognizing that the consent inquiry hinges on whether the Plaintiffs’ expectations  
5 were objectively reasonable, Yelp next argues that the Plaintiffs did not have to understand that  
6 their contacts data would be uploaded to Yelp’s servers in order to effectively consent to the  
7 Friend Finder function. ECF No. 759 at 14-15. In other words, Yelp argues that “consent to [the  
8 Friend Finder] process does not require the user to understand how the process works.” Id. After  
9 all, Yelp argues, “[w]e consent to all sorts of things every day without the slightest idea how they  
10 are accomplished.” Id.

11 But the details about how the process works matter to the consent analysis if those details  
12 involve conduct that transcends what was consented to and interferes with the Plaintiffs’  
13 objectively reasonable expectations of privacy. Shulman, 18 Cal. 4th at 232. Here, the Plaintiffs  
14 have presented evidence that the act of uploading their contacts’ email addresses without their  
15 permission changed the nature of Yelp’s intrusion. For example, one of the Plaintiffs testified that  
16 she “gave Yelp permission to access [her] contacts,” but not to “upload [her] contacts on to their  
17 servers.” Depo. Tr. of Claire Hodgins, ECF No. 759-3 at 106:23-107:5. She further testified that  
18 uploading the data was qualitatively different than accessing it because “uploading means that you  
19 can then use that information how you please.” ECF No. 777-3 at 5:7-12. Other Plaintiffs  
20 testified that the act of uploading the contacts data to a server was “egregious,” and that they  
21 didn’t consent to Yelp “taking” their information by moving it from their phone to somewhere  
22 else. Depo. Tr. of Nirali Mandalaywala, ECF No. 777-2 at 7:5-18; Depo. Tr. of Giuliana Biondi,  
23 ECF No. 777-4 at 3:18-4:4. It remains to be seen whether these expectations were objectively  
24 reasonable, but that is a question for the jury, not this Court. See Shulman, 18 Cal. 4th at 233-34  
25 (reversing the lower court’s grant of summary judgment as to the plaintiff’s intrusion upon  
26 seclusion claim because the determination as to whether the plaintiff’s expectation of privacy was  
27 reasonable was a “question[] for the jury”).

**B. Highly Offensive**

Next, Yelp argues that the Plaintiffs cannot succeed on their intrusion upon seclusion claim as a matter of law because “identifying social connections to users is far from a ‘highly offensive’ practice.” ECF No. 689 at 17:14-15.

To prevail on an invasion of privacy claim, the intrusion must also be “highly offensive to a reasonable person and sufficiently serious and unwarranted as to constitute an egregious breach of the social norms.” Hernandez v. Hillsides, Inc., 47 Cal. 4th 272, 295 (2009) (internal citations and quotation marks omitted). “A court determining the existence of ‘offensiveness’ would consider the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder’s motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded.” Miller v. Nat’l Broad. Co., 187 Cal. App. 3d 1463, 1483-84 (Ct. App. 1986). “California tort law provides no bright line on [offensiveness]; each case must be taken on its facts.” Hernandez, 47 Cal. 4th at 1073 (quoting Shulman, 18 Cal. 4th at 237) (internal quotation marks omitted). “[W]hat is ‘highly offensive to a reasonable person’ suggests a standard upon which a jury would properly be instructed.” Deteresa v. Am. Broad. Companies, Inc., 121 F.3d 460, 465 (9th Cir. 1997) (quoting Miller, 187 Cal. App. 3d at 1483). However, “there is a preliminary determination of ‘offensiveness’ which must be made by the court in discerning the existence of a cause of action for intrusion.” Id. “If the undisputed material facts show no reasonable expectation of privacy or an insubstantial impact on privacy interests, the question of invasion may be adjudicated as a matter of law.” Id. (internal citations and quotation marks omitted).

Yelp argues that “mechanical access to a list of email addresses in order to perform a commonplace social media function is far short of conduct that shocks the conscience, or so transgresses social norms that it can be deemed outrageous” and that “such commercial uses of address information are not ‘highly offensive.’” ECF No. 689. In other words, Yelp argues that uploading address book data without users’ consent is not highly offensive because it is “commonplace” and “commercial” in nature. Id. at 17:17-18.

Yelp relies heavily on Folgelstrom v. Lamps Plus, Inc., 195 Cal. App. 4th 986 (2011), as

1 modified (June 7, 2011), to support its argument. In Folgelstrom, a California appellate court held  
2 that the retailer's practice of asking for a customer's zip code and then trading the customer's  
3 information with a third party credit reporting agency in exchange for the customer's full mailing  
4 address so that it could send the customer promotional materials was not highly offensive.  
5 Folgelstrom, 195 Cal. App. 4th at 989, 993 ("However questionable the means employed to obtain  
6 plaintiff's address, there is no allegation that Lamps Plus used the address once obtained for an  
7 offensive or improper purpose."). In reaching this conclusion, the court explained that it had  
8 "found no case which imposes liability based on the defendant obtaining unwanted access to the  
9 plaintiff's private information which did not also allege that the *use* of plaintiff's information was  
10 highly offensive." Id. at 993. Yelp relies on Folgelstrom to argue that the subsequent *use* of any  
11 private information obtained—and not just the initial intrusion itself—must be highly offensive to  
12 succeed on an intrusion upon seclusion claim, and that "commercial uses of address information  
13 are not highly offensive." Id. at 16-18.

14 Yelp's reliance on Folgelstrom is not persuasive. The offensiveness inquiry is fact-  
15 specific, and this Court has already distinguished Folgelstrom because the data at issue here is  
16 "more private than a person's mailing address" and this kind of intrusion is not "routine  
17 commercial behavior." ECF No. 471 at 47-48. For the same reason, the Court is not persuaded by  
18 cases that have mechanically applied Folgelstrom to invasion of privacy claims. See, e.g., In re  
19 iPhone Application Litig., 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012); In re Google, Inc.  
20 Privacy Policy Litig., 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014).

21 In re iPhone Application Litig. involved the disclosure to third parties of an iDevice user's  
22 unique device identifier number, personal data, and geolocation information. 844 F. Supp. 2d at  
23 1063. That court held without explanation that "[e]ven assuming this information was transmitted  
24 without Plaintiffs' knowledge and consent, a fact disputed by Defendants, such disclosure does not  
25 constitute an egregious breach of social norms," citing Folgelstrom. Id. As noted above,  
26 however, Folgelstrom addressed different facts than those in iPhone Application Litigation, and  
27 the latter court did not explain how expansion of Folgelstrom's holding, counter to the privacy  
28 interests of iDevice users, was consistent with California's community privacy norms.

1       The reasoning in In re Google, Inc. Privacy Policy Litig. is also unhelpful. In that case,  
2 plaintiffs challenged a Google privacy policy that allowed Google to comingle user data across  
3 accounts and disclose it to third-parties for advertising purposes. In re Google, Inc. Privacy Policy  
4 Litig., 58 F. Supp. 3d at 974. Noting that “[t]his district ‘set[s] a high bar’ for the requisite  
5 ‘intrusion [that is] highly offensive to a reasonable person,’” the court held that “In re iPhone  
6 Application Litig.’s analogous facts . . . teach here that Plaintiffs’ allegations do not plausibly rise  
7 to the level of intrusion necessary to establish an intrusion claim.” Id. at 988 (quoting Belluomini  
8 v. Citigroup Inc., Case No. 3:13-cv-01743, 2013 WL 5645168, at \*3 (N.D.Cal. Oct. 16, 2013)).  
9 Again, however, the court in Google made no effort to explain why Google’s practices were  
10 consistent with community notions of privacy as they existed at the time of the decision. Because  
11 In re iPhone Application Litig. relied on an overreading of Folgelstrom, as set forth above, and  
12 Google in turn rests entirely In re Phone Application Litig., it too is unhelpful here.<sup>9</sup>

13       Fundamentally, this case is about whether Apple’s conduct and that of application  
14 developers violated community norms of privacy. “A ‘reasonable’ expectation of privacy is an  
15 objective entitlement founded on broadly based and widely accepted community norms.” Hill, 7  
16 Cal.4th at 37. The “community norms” aspect of the “reasonable expectation of privacy” element  
17 means that “[t]he protection afforded to the plaintiff’s interest in his privacy must be relative to  
18 the customs of the time and place, to the occupation of the plaintiff and to the habits of his  
19 neighbors and fellow citizens.” In re Yahoo Mail Litig., 7 F. Supp. 3d 1016, 1038 (N.D. Cal.  
20 2014) (quoting TBG Ins. Servs. Corp. v. Superior Court, 96 Cal. App. 4th 443, 450, (2002)).

21       Those customs and habits are very much in flux. The technology underlying the  
22 allegations in this case is still developing. The iPhone was introduced less than ten years ago,  
23 Charles Arthur, “The History of Smartphones: Timeline,” Guardian UK Jan. 24, 2012 (on-line ed)  
24 (<https://www.theguardian.com/technology/2012/jan/24/smartphones-timeline>), and the prospect of

25 \_\_\_\_\_  
26 <sup>9</sup> Yelp also cites Puerto v. Super. Ct., 158 Cal. App. 4th 1242, 1253–54 (2008) for the proposition  
27 that “contact information is not ‘particularly sensitive’ and is not the type of information deemed  
28 ‘private.’” ECF No. 689 at 12. Puerto concerned the discovery of absent class member contact  
information and has nothing to do with intrusion on seclusion claims.

1 an application developer taking advantage of a user's contacts data is even newer still. When  
2 applying community standards, it is possible that a jury of persons selected from that community  
3 might conclude, as Yelp suggests, that Yelp's conduct was "far from "highly offensive." ECF No.  
4 689 at 11. In the alternative, a jury might also find the intrusion highly offensive based on both  
5 the degree of intrusion (uploading the email addresses of a user's contacts to the Defendants'  
6 servers) and the setting in which the invasion took place (users' personal cellular phones). Miller,  
7 187 Cal. App. 3d at 1483-84.<sup>10</sup> Perhaps a democratically elected legislature will embody the  
8 community standards in a statute. In any of those events, a jury or legislature will have performed  
9 an important function in reflecting the community's standards as they relate to the privacy of  
10 information stored on a user's smartphone. A judge should be cautious before substituting his or  
11 her judgment for that of the community.

12 In sum, this is not – or is not yet – a question that can be decided as a matter of law, and  
13 there is a triable issue of fact regarding whether Yelp's upload of the Plaintiffs' address book data  
14 was highly offensive to a reasonable person.

15 **C. Copyright Act Preemption**

16 Finally, Yelp argues that under the Plaintiffs' theory its "copying of the Plaintiffs' contact  
17 information becomes the *only* act alleged against Yelp" such that the claim is preempted by the  
18 Copyright Act. ECF No. 689 at 19-20.

19 The Copyright Act preempts a state law claim if: (1) the plaintiff asserts "rights that are  
20 equivalent" to those protected by the Copyright Act as defined in 17 U.S.C. § 106; and (2) the  
21 work involved falls within the "subject matter" of the Copyright Act as defined in 17 U.S.C. §§  
22 102 and 103. Kodadek v. MTV Networks, Inc., 152 F.3d 1209, 1212 (9th Cir. 1998).

23 Assuming the collection of email addresses falls within the "subject matter" of the  
24 Copyright Act,<sup>11</sup> the Plaintiffs' state law privacy rights are nonetheless qualitatively different from  
25

---

26 <sup>10</sup> The sheer volume of media attention surrounding the app developers' conduct, and the fact that  
27 both Congress and a federal agency initiated investigations, are some evidence of the existence of  
developing social norms surrounding this technology.

28 <sup>11</sup> Yelp argues that the address book data is a "literary work" that falls within the subject matter of  
copyright. ECF No. 689 at 20. Although Yelp concedes that the collection of email addresses

1 the rights protected by the Copyright Act. “A right is ‘equivalent’ to copyright if it ‘is infringed  
2 by the mere act of reproduction, performance, distribution or display.’” Entous v. Viacom Int’l,  
3 Inc., 151 F. Supp. 2d 1150, 1159 (C.D. Cal. 2001) (quoting Nimmer on Copyright, § 1.10[B] at 1–  
4 12 to 1–13 (1989)). However, a state law claim is not “equivalent” to rights within the scope of  
5 copyright if it “contains an additional element not required for a copyright claim.” Ryan v.  
6 Editions Ltd. W., Inc., 786 F.3d 754, 760 (9th Cir.), cert. denied, 136 S. Ct. 267, 193 L. Ed. 2d  
7 136 (2015); see also Montz v. Pilgrim Films & Television, Inc., 649 F.3d 975, 981 (9th Cir. 2011)  
8 (holding that a claim for breach of confidence “protects the duty of trust or confidential  
9 relationship between the parties, an extra element that makes it qualitatively different from a  
10 copyright claim.”)

11 As explained in § 106, the Copyright Act grants exclusive rights to reproduce the  
12 copyrighted work, prepare derivative works, distribute copies to the public, and perform or display  
13 the copyrighted work publicly. Laws v. Sony Music Entm’t, Inc., 448 F.3d 1134, 1143, n. 3 (9th  
14 Cir. 2006) (quoting 17 U.S.C. § 106). In contrast, the Plaintiffs’ state law privacy claim protects  
15 the Plaintiffs’ rights to be free from highly offensive and unwarranted intrusions into a private  
16 sphere. Shulman, 18 Cal. 4th at 231. This “extra element”—using the Plaintiffs’ data in a highly  
17 offensive way that intrudes into an area that they reasonably expect to remain private—changes  
18 the nature of the action. In this case, the Plaintiffs do not allege that Yelp violated their privacy  
19

---

20 “likely does not qualify for copyright protection,” it correctly points out that this does not preclude  
21 preemption. Id.; see also Firoozye v. Earthlink Network, 153 F. Supp. 2d 1115, 1124–25 (N.D.  
22 Cal. 2001) (explaining that “the subject matter of copyright is broader than copyright protection”  
23 and, therefore, the relevant question for the purpose of copyright preemption is not whether the  
24 work is actually copyrightable, but rather “whether the work involved is a kind of work that comes  
25 within the subject matter of the Copyright Act”). Because factual compilations like the address  
26 book data at issue here may be copyrightable in some instances, the Court assumes that the data  
27 falls within the subject matter of the Copyright Act. See Feist Publications, Inc. v. Rural Tel.  
28 Serv. Co., 499 U.S. 340, 348–49 (1991) (acknowledging “thin” copyright protection for factual  
compilations—in that case, a telephone directory—to the extent that the author’s selection and  
arrangement of those facts was original and “entail[ed] a minimal degree of creativity”); Firoozye,  
153 F. Supp. 2d at 1124–25 (“[M]aterial that falls within a category that is eligible for protection  
in certain instances must come within the Act’s subject matter.”). Regardless, the Court holds that  
the other requirement for copyright preemption is not satisfied.

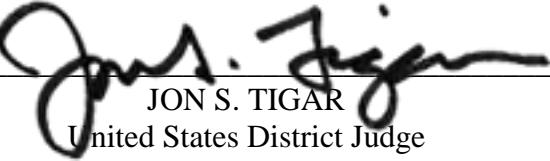
1 rights by simply reproducing or copying the address book data, but rather by uploading their  
2 address book data to Yelp's servers to be analyzed against the database of existing Yelp users  
3 without their permission. Because this privacy claim alleges conduct that transcends the mere act  
4 of copying or reproducing the Plaintiffs' work, the Plaintiffs' claim is simply not "equivalent" to  
5 rights protected under copyright law. Therefore, the claim is not preempted by the Copyright Act.

6 **CONCLUSION**

7 In conclusion, there are genuine issues of material fact as to both the scope of the consent  
8 that Yelp obtained and whether uploading the Plaintiff's address book data remained within that  
9 scope. Accordingly, the Court denies Yelp's motion for summary judgment.

10 IT IS SO ORDERED.

11 Dated: September 8, 2016

12   
13 JON S. TIGAR  
14 United States District Judge

United States District Court  
Northern District of California

15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28