Jay Edelson (Admitted *pro hac vice*)
jedelson@edelson.com
EDELSON PC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

Shawn A. Williams (213113)
shawnw@rgrdlaw.com
ROBBINS GELLER RUDMAN & DOWD LLP
Post Montgomery Center
One Montgomery Street, Suite 1800
San Francisco, California 94104
Tel: 415.288.4545
Fax: 415.288.4534

Paul J. Geller (Admitted *pro hac vice*)
pgeller@rgrdlaw.com
ROBBINS GELLER RUDMAN & DOWD LLP
120 East Palmetto Park Road, Suite 500
Boca Raton, Florida 33432
Tel: 561.750.3000
Fax: 561.750.3364

Joel H. Bernstein (Admitted *pro hac vice*)
jbernstein@labaton.com
LABATON SUCHAROW LLP
140 Broadway
New York, New York 10005
Tel: 212.907.0700
Fax: 212.818.0477

Counsel for In re Facebook Biometric Info. Plaintiffs and the Putative Class

[Additional counsel appear on the signature page.]

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

In re Facebook Biometric Information Privacy Litigation

THIS DOCUMENT RELATES TO:
ALL ACTIONS

Master Docket No. 3:15-cv-3747-JD

PLAINTIFFS' RESPONSE IN OPPOSITION TO FACEBOOK'S RENEWED MOTION TO DISMISS FOR LACK OF SUBJECT MATTER JURISDICTION

Date: November 30, 2017
Time: 10:00 a.m.
Location: Courtroom 11

Hon. James Donato

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutory Authority

Constitutional Provisions

INTRODUCTION

In these actions, Plaintiffs seek redress for Facebook's unlawful collection of their biometric data in violation of Illinois' Biometric Information Privacy Act, 740 ILCS 14/1 *et seq.* ("BIPA"). Having failed in its bid to deny Illinois consumers the protection of their state's biometric privacy regime based on a choice of law clause in a contract of adhesion, Facebook now tries a different tactic to usurp those same rights and negate the fundamental public policy of the state. Although this Court correctly pointed out that the Ninth Circuit's decision in *Robins v. Spokeo, Inc.*, 867 F.3d 1108 (9th Cir. 2017), did not go Facebook's way, (dkt. 222 at 10:10-12), Facebook nevertheless has brought yet another motion in which it argues that Article III of the United States Constitution prohibits the Court from hearing this case.

Facebook relies on the *Spokeo* opinion that it wishes it had gotten, not the one that actually came down. Parroting the language in defendant Spokeo's briefing (but not the language of the Ninth Circuit or the Supreme Court), Facebook contends that Plaintiffs lack standing because they have not suffered what Facebook calls "real-world harm." Despite directives to the contrary from both the Supreme Court and the Ninth Circuit, it insists that in the context of a claim for statutory damages, a plaintiff must always "allege[] a statutory violation *plus* a harmful result" to meet Article III's requirement of a concrete injury-in-fact. *Compare* dkt. 227 at 8-9 *with Spokeo*, 867 F.3d at 1113 ("[T]he Supreme Court also recognized that *some* statutory violations, alone, do establish concrete harm.").

There are two questions this Court must answer to determine whether Plaintiffs' injuries were concrete under Article III: "(1) whether the statutory provisions at issue were established to protect [their] concrete interests (as opposed to purely procedural rights), and if so, (2) whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests." *Spokeo*, 867 F.3d at 1113. The answer to the first question is "yes" because, as the Court has already determined, BIPA's privacy protections represent the strong policy of Illinois, not a purely procedural right. The answer to the second question is also "yes" because Facebook's unlawful collection of Plaintiffs' biometric information invades the interest that Illinois sought to protect when it passed BIPA. Accordingly, Plaintiffs have standing and the

Court has jurisdiction. And although Facebook insists that Plaintiffs consented to collection of their biometric information, the purported notice does not even mention faceprints or any other biometric information. That said, if the Court were to determine that it lacked jurisdiction, then the case Facebook removed from Illinois state court would have to be remanded, not dismissed.

ARGUMENT

I. The Court Has Already Recognized that BIPA Protects an Important, Concrete Interest: The Right to Privacy In Personal Biometric Data.

As the Ninth Circuit recognized in *Spokeo*, the Court must first determine whether BIPA protects a concrete interest. As the Court pointed out at the argument on Facebook's first *Spokeo* motion, that issue has effectively already been decided. (Dkt. 167 at 6-7.) Facebook initially sought dismissal of this case on the grounds that a contractual choice-of-law clause required the application of California law, which prevented Illinois Facebook users from vindicating their Illinois statutory rights. This Court rejected that view and Facebook's application of the California choice-of-law clause, holding that "[t]here can be no reasonable doubt that the Illinois Biometric Information Privacy Act embodies a fundamental policy of the state of Illinois." (Dkt. 120 at 17.) "By its express terms, BIPA manifests Illinois' *substantial policy* of protecting its citizens' right to privacy in their personal biometric data." *Id.* (emphasis added). If BIPA protected "purely procedural rights," *see Spokeo*, 867 F.3d at 1113, then it could hardly be the kind of substantial policy that warrants overriding a contractual choice-of-law clause. This Court's previous holding, therefore, cannot be reconciled with Facebook's position that Plaintiffs have not identified a concrete interest.

Facebook now seeks reconsideration through the back door, contending that "[c]ourts have been willing to entertain privacy-related lawsuits only when they implicate *specific* privacy interests … that bear directly on a person's livelihood, reputation, or mental state." (Dkt. 227 at 6) (emphasis in original). The defendant in *Spokeo* tried to advance much the same position before the Ninth Circuit without any success. In that case the plaintiff, Thomas Robins, had standing to sue the Defendant, Spokeo, under the Fair Credit Reporting Act for having prepared and published a credit report about him that included incorrect information about his age,

education, and level of wealth. *Spokeo*, 867 F.3d at 1111. Facebook contends that in its holding, the Ninth Circuit "relied heavily" on Robins's allegations that he was out of work or that he had suffered from anxiety or other emotional distress. (Dkt. 227 at 8.) In fact, the opposite is true. Although Spokeo tried to push that view, the court rejected it:

> Spokeo argues that, at best, Robins has asserted that such inaccuracies might hurt his employment prospects, but not that they present a material or impending risk of doing so. … Here … both the challenged conduct and the attendant injury have already occurred. As alleged in the complaint, Spokeo has indeed published a materially inaccurate consumer report about Robins. And, as we have discussed, the alleged intangible injury caused by that inaccurate report has also occurred. We have explained why, in the context of FCRA, this alleged intangible injury is itself sufficiently concrete. **It is of no consequence how likely Robins is to suffer *additional* concrete harm as well (such as the loss of a specific job opportunity).**

Spokeo, 867 F.3d at 1118 (bold emphasis added).

The same logic applies to privacy cases. In *Van Patten v. Vertical Fitness Group, LLC*, 847 F.3d 1037, 1043 (9th Cir. 2017), the Ninth Circuit considered the Telephone Consumer Protection Act—a privacy statute. The plaintiffs in that case had standing not because their livelihood or reputation or mental state were affected by the defendant's violation of the statute, and not because some private information about them was disclosed without permission, but because they suffered the "unwanted intrusion and nuisance of unsolicited telemarketing phone calls[.]" *Id.* at 1043. Facebook does not and cannot explain why that invasion of privacy is somehow more "specific" than the invasion of privacy suffered by Plaintiffs when Facebook secretly collected their sensitive, personal biometric information. Indeed, the last time Facebook brought a motion to dismiss based on *Spokeo*, the Court suggested that "getting an unwanted text on your cell phone seems to me to be several steps away from, in terms of being much more mild, than having your biometrics harvested and used without your permission." (Dkt. 167 at 10:4-7.)

Facebook also relies on instances where plaintiffs lacked standing because they brought statutory claims involving "the retention of information lawfully obtained[.]" *Braitberg v. Charter Commc'ns, Inc.*, 836 F.3d 925, 930 (8th Cir. 2016). *See also Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909 (7th Cir. 2017) (discussing standing in the context of improperly

retained but properly collected cable viewing history); *Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 514 (D.C. Cir. 2016) (holding that disclosure of a zip code was not a concrete injury). But here, Facebook did not obtain Plaintiffs' biometric information lawfully. In the statutes at issue in *Braitberg*, *Gubala*, and *Hancock*, Congress did not regulate, or even consider, the collection of the regulated information in question.[1] By contrast, the purpose of BIPA is to proscribe the unauthorized collection of biometric information because "biometrics are unlike other unique identifiers. They're totally special," and if they're compromised, then "the individual has no recourse[.]" (Dkt. 167 at 8:3-5.) That is why the "Illinois Legislature has been very specific about saying, *Your biometrics are yours, and yours alone; and if they're going to be harvested, you have the right to make sure they're harvested with your consent. And if that doesn't happen, you have been concretely injured*." (*Id.* at 8:9-14) (italics in original).

A review of the legislative history confirms the accuracy of the Court's statement. BIPA was sparked by an incident in which a company had collected a consumers' biometric data, and, when the company went into bankruptcy, it became clear that consumers were unaware of exactly who had collected their data and what that company was allowed to do with it. (*See* dkt. 70-2.) To solve this problem, the Legislature required entities collecting biometric identifiers to get consent first, as well as to tell consumers exactly what they planned to do with the identifiers and how long they planned to keep it. 740 ILCS 14/15. BIPA, therefore, "is premised on the Illinois legislature's stated concerns about the use of new technology … to *collect* personal biometric data." (Dkt. 120 at 17) (emphasis added). Unlike the information at issue in *Braitberg*,

[1] Facebook contends "[c]ourts have been willing to entertain privacy-related lawsuits only when they implicate . . . 'untruthful disclosures' [or] 'dissemination of private information,'" but not "mere *collection*." (Dkt. 227 at 6-7.) That's not true. *See, e.g.*, *Satchell v. Sonic Notify, Inc.*, 234 F. Supp. 3d 996, 1005 (N.D. Cal. 2017) (that Defendants "***captured*** . . . private conversations without [Plaintiff's] knowledge or consent . . . sufficient to demonstrate she suffered injury-in-fact."); *Matera v. Google Inc.*, No. 15-cv-04062, 2016 WL 5339806, at *14 (N.D. Cal. Sept. 23, 2016) ("unauthorized ***interception*** of communication constitutes cognizable injury"); *Rackemann v. LISNR, Inc.*, No. 17-cv-624, 2017 WL 4340349, at *4 (S.D. Ind. Sept. 29, 2017) ("surreptitiously ***accessing*** the private communications of another" sufficient for injury-in-fact); *Osgood v. Main Streat Mktg., LLC*, No. 16-cv-2415, 2017 WL 131829, at *7-8 (S.D. Cal. Jan. 13, 2017) (***recording*** calls without consent constitutes "an invasion of privacy injury which is sufficient to confer Article III standing under *Spokeo*") (all emphasis added).

Gubala, and *Hancock*, biometric information is so sensitive that even collecting it substantially affects individuals' privacy interest. *See Friedman v. Boucher*, 580 F.3d 847, 859 (9th Cir. 2009) (holding that government's taking of a DNA sample without consent violates the Fourth Amendment); *see also In re May 1991 Will Cty. Grand Jury*, 604 N.E.2d 929, 935 (Ill. 1992). By regulating on the front end and allowing consumers to enforce their right not to have their faceprints collected without consent, the legislature protected consumers' concrete privacy interest in controlling who is collecting their biometric information and for what purpose.[2]

II. Facebook's Secret Collection of Plaintiffs' Biometric Information Creates a Material Risk of the Harm Identified by the Illinois Legislature.

Second, the violations that Plaintiffs allege do harm or, at the very least, present a material risk of harm to the interests that the Illinois legislature was trying to protect. In *Spokeo*, the Ninth Circuit considered this issue by looking at what interests Congress intended to protect when it passed the FCRA. After concluding that "the FCRA procedures at issue in this case were crafted to protect consumers' … concrete interest in accurate credit reporting about themselves," the Ninth Circuit went on to examine "the *nature* of the specific alleged reporting inaccuracies to ensure that they raise a real risk of harm to the concrete interests that FCRA protects." *Spokeo*, 867 F.3d at 1115-16. It explained that while certain trivial inaccuracies might not raise such a risk, the inaccuracies of the type that the plaintiff raised in his complaint certainly did. *See id.* at 1117.

The question is not, therefore, whether Facebook's unauthorized secret collection of their biometric information "caus[ed] them emotional harm or … materially affect[ed] their reputations, livelihoods, or relationships." (Dkt. 227 at 10.) The question is whether Plaintiffs' allegations are "trivial" or whether they "raise a risk of real harm to the concrete interests" that

[2] The Court signaled at a previous hearing that BIPA's relationship to the common law was not relevant to standing in this case. (Dkt. 167 at 28.) ("So the fact that this cannot be traced to something in the 18th Century is not, in my view, even relevant."). Nevertheless, for the sake of completeness, Plaintiffs note that "[a]ctions to remedy defendants' invasions of privacy, intrusion upon seclusion, and nuisance have long been heard by American courts, and the right of privacy is recognized by most states," *Van Patten*, 847 F.3d at 1043, including Illinois, *see Leopold v. Levin*, 259 N.E.2d 250, 253-54 (Ill. 1970).

BIPA protects. *See Spokeo*, 867 F.3d at 1116.

Spokeo did not change the long standing rule that state legislatures are permitted to "articulat[e] a chain[ ] of causation that will give rise to a case or controversy." *Syed v. M-I, LLC*, 853 F.3d 492, 499 (9th Cir. 2017) (internal quotation marks omitted). For example, even though Congress's concern about inaccurate credit reports had do to with the potential effect of those reports on employment decisions and loan applications, a plaintiff does not need to have suffered those effects to have standing. *Spokeo*, 867 F.3d at 1114, 1117. Thus, the plaintiff in *Spokeo* had standing to sue for the inaccuracies in his credit report "[e]ven if their likelihood actually to harm [his] job search could be debated." *Id.* at 1117.

Likewise, Plaintiffs have standing here because they have alleged sufficient facts for the Court to conclude that Facebook's unauthorized collection of their biometric information "seems directly and substantially related to [BIPA]'s goals." *See id*. As discussed above, the interest that BIPA protects is consumers' right to keep control of their private biometric information. The legislature identified a number of harms that could stem from the unauthorized collection of such information, including consumers' reluctance or inability to adopt biometric technology when they find out, after the fact, that their biometric information has been collected. 740 ILCS 14/5(c). Further, it noted the high severity of those harms—they leave the individual with "no recourse[.]" *Id.*

It is perhaps true (although by no means settled) that certain violations of BIPA might be so trivial that they cannot possibly cause a material risk of those harms. For example, in *McCollough v. Smarte Carte, Inc.*, No. 16 C 03777, 2016 WL 4077108, at *1 (N.D. Ill. Aug. 1, 2016), users rented storage lockers by "plac[ing] their finger on a fingerprint scanner, which [was] then displayed on the screen." While the defendant did not get the proper informed consent to collect that information, the plaintiff knew at the very least that his fingerprint was being collected and who was collecting it, which leads to questions regarding whether he had actually suffered a material risk of harm. It is far from settled that the *McCollough* court's analysis is correct, especially considering that it relies on the premise that "a state statute cannot confer federal constitutional standing," 2016 WL 4077108, at *5, which contravenes both Seventh and

Ninth Circuit authority, *see Cantrell v. City of Long Beach*, 241 F.3d 674, 684 (9th Cir. 2001) ("We agree with the Seventh Circuit that state law can create interests that support standing in federal courts.") (citing *FMC Corp. v. Boesky*, 852 F.2d 981, 992 (7th Cir. 1988)).

But Facebook's "scan of face geometry … done without plaintiffs' consent," (dkt. 120 at 22), is not a trivial violation. As another court in the same district found, the *McCollough* analysis does not make sense where users do not know that their biometric information is being collected. In *Monroy v. Shutterfly Inc.*, the plaintiff alleged that the defendant, an online photo-sharing service, had collected his faceprint without permission from photographs that he had uploaded. No. 16-cv-10984, 2017 WL 4099846, at *1 (N.D. Ill. Sept. 15, 2017). Considering the Article III standing issue, the *Monroy* court distinguished both *McCollough* and the other district court case that Facebook relies upon:

> [T]he facts alleged in this case differ significantly from those alleged in *McCollough* and *Vigil*. In the latter cases, the plaintiffs voluntarily provided their biometric data to the defendants. The plaintiff in *McCollough* had rented one of the defendant's electronic storage lockers, which were locked and unlocked using customers' fingerprints on a touchscreen. In *Vigil*, the plaintiffs voluntarily had their faces scanned to create personalized avatars for use in a videogame. The harm alleged in the latter cases was the defendants' failure to provide them with certain disclosures (e.g., that their biometric data would be retained for a certain length of time after it had been obtained). **Monroy, by contrast, alleges that he had no idea that Shutterfly had obtained his biometric data in the first place**. Thus, in addition to any violation of BIPA's disclosure and informed consent requirements, Monroy also credibly alleges an invasion of his privacy.

Id. at *8 n.5 (emphasis added).[3]

Here, Plaintiffs allege the same thing as the plaintiff in *Monroy*: "Without even informing its users – let alone obtaining their informed written consent – Facebook through Tag

[3] The *Vigil* decision was also plainly erroneous. The *Vigil* court erred right out of the gate by misidentifying the concrete interest underlying BIPA as data protection rather than biometric privacy. *Compare Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499, 510-511 (S.D.N.Y. 2017) (mistaking BIPA's "core object" as "data protection to curb potential misuse of biometric information") *with* dkt. 120 at 21-22 (noting BIPA's "broad purpose of protecting privacy in the face of emerging biometric technology") *and Rivera v. Google Inc*., 238 F. Supp. 3d 1088, 1096 (N.D. Ill. 2017) ("It is not the [method of collection or use] that is important to [BIPA]; what's important is the potential ***intrusion on privacy posed by the unrestricted gathering of biometric information***.") (emphasis added).

Suggestions automatically … extracted biometric identifiers from their uploaded photographs and previously tagged pictures, and stored these biometric identifiers in a database." (Dkt. 40 ¶ 26.) That unlawful extraction and collection of Plaintiffs' biometric information is not trivial. To the contrary, it is exactly what the Illinois Legislature was trying to prevent when it passed BIPA, constitutes an invasion of Plaintiffs' privacy, and is a concrete injury in fact. (*See* dkt. 40 ¶ 66) ("By collecting, storing, and using Plaintiffs' and the Class's biometric identifiers as described herein, Facebook violated Plaintiffs' and the Class's rights to privacy in their biometric identifiers as set forth in the BIPA[.]").

III. Plaintiffs Did Not Consent to Collection of Their Biometric Information.

As a last-ditch effort, Facebook contends that its failure to comply with BIPA's notice and consent provisions was merely "technical" because its Data Policy vaguely references collection of information. But a key purpose of BIPA is to make sure that Illinois consumers know who has their immutable biometric information and what it is being used for. Facebook's argument would eviscerate the statute, which is "an *informed consent* privacy law[.]" (Dkt. 120 at 21) (emphasis added). Here, Facebook does not even come close to obtaining informed consent.

Facebook's argument relies on its Data Policy, which it says is part of its user agreement (although it refers to a version dated months after this complaint was filed). The first section of that document is entitled "What kinds of information do we collect?" and details what Facebook means throughout policy when it refers to "information." In the copy of that policy provided to the Court, Facebook's counsel literally obscures the critical first section by artfully covering it up with a dialog box.[4] (*See* dkts. 227-2, 227-3.) The obscured portion of the policy relates specifically to what type of information Facebook collects from photographs uploaded by users, and it notes that the collected information about photographs "can include information in or about the content you provide, such as the location of a photo or the date a file was created." (Declaration of Rafey S. Balabanian, Ex. A ["Data Policy"], § I.) Neither that portion of the

[4] This inaccuracy likely violates the Court's standing order. *See* Standing Order for Civil Cases Before Judge James Donato, ¶ 23.

policy dealing specifically with photographs or any other portion of the policy says *anything* about collection of faceprints or any other biometric identifier. It does not tell users of the fact that Facebook is collecting biometric information or why it is collecting the information. It simply cannot be said that the policy puts users on notice that Facebook will collect their faceprints. And, Facebook's oblique, incomplete disclosures do not satisfy the specific informed written consent required under BIPA. *See Syed*, 853 F.3d at 499-500 (even where Plaintiff received some of the required disclosure, the defendants' deficient disclosure violated the plaintiff's statutory privacy rights and thus sufficed to constitute concrete injury-in-fact).

If users are somehow able to figure out that Facebook is collecting biometric information, the absence of any reference to biometric information in the Data Policy makes it impossible for them to tell what Facebook is doing with that information. The Data Policy includes an entire section on how different categories of information are shared: Facebook purports to keep some types of information to itself, and it shares other information with third parties and advertisers. (Data Policy § III.) But because the Data Policy does not reference biometric information, it is impossible to know what category it falls under. Similarly, the Data Policy says that certain information is deleted when users delete their accounts, but again it is impossible to tell whether biometric information falls into this category. (*Id.* § IV.)

The Data Policy therefore exemplifies the *exact problem* that the Illinois legislature was trying to remedy when it passed BIPA. Facebook is collecting users' biometric information without telling them, which causes them to lose control over that information. If consumers do figure out that Facebook is collecting the information, they still have no idea what Facebook is doing with it or whom else it is sharing the information with. The "consent" that Facebook says it obtained is nowhere close to the kind of informed consent that that Illinois legislature determined is absolutely required to protect consumers' privacy interests.

IV. If There Is a Question about Federal Jurisdiction, Licata's Case Must Be Severed and Remanded to Illinois State Court.

Finally, Facebook removed one of the consolidated cases—that of Plaintiff Carlo Licata—from the Circuit Court of Cook County, Illinois to the United States District Court for

the Northern District of Illinois, after which it was transferred to this Court. *See* Facebook's Notice of Removal, *Licata v. Facebook, Inc.*, No. 1:15-CV-04022, dkt. 1 (N.D. Ill. May 6, 2015). As explained in detail above, there is no real question that Licata has Article III standing here, since he has unambiguously suffered an injury in fact.

However, should the Court determine that it is a close question, then there is no need to decide whether Licata has properly alleged such an injury. *See Hunter v. Philip Morris USA*, 582 F.3d 1039, 1042 (9th Cir. 2009) (holding that in line with the "strong presumption against removal jurisdiction[,] … the court resolves all ambiguity in favor of remand to state court."). Instead, per 28 U.S.C. § 1447(c), his case must be severed and remanded to Cook County. *Albingia Versicherungs A.G. v. Schenker Int'l Inc.*, 344 F.3d 931, 938 (9th Cir.), *opinion amended and superseded on denial of reh'g,* 350 F.3d 916 (9th Cir. 2003) ("[S]ection 1447(c) means that if it is discovered at any time in the litigation that there is no federal jurisdiction, a removed case must be remanded to the state court rather than dismissed."); *Langford v. Gates*, 610 F. Supp. 120, 122-23 (C.D. Cal. 1985) (lack of standing is a jurisdictional defect, and "the proper course is remand" under § 1447(c), "not dismissal"). Although Facebook's motion requests dismissal of the complaints for lack of subject-matter jurisdiction, (dkt. 227 at 12), it has already conceded that if it is correct that the Court lacks jurisdiction, Licata's case would have to be remanded, (dkt. 167 at 29:14-18.) There should thus be no disagreement among the parties on this point.

CONCLUSION

Facebook's renewed motion to dismiss should be denied because the Court unquestionably has subject-matter jurisdiction over this action. Notwithstanding, if the Court should determine that it lacks jurisdiction, then Licata's case must be severed and remanded to the Circuit Court of Cook County, Illinois.

Respectfully submitted,

ADAM PEZEN, **CARLO LICATA**, and **NIMESH PATEL**, individually and on behalf of all others similarly situated,

Dated: October 26, 2017

By: /s/ Rafey S. Balabanian
One of Plaintiffs' Attorneys

Jay Edelson (Admitted *pro hac vice*)
jedelson@edelson.com
Alexander G. Tievsky (Admitted *pro hac vice*)
atievsky@edelson.com
EDELSON PC
350 North LaSalle Street, 13th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

Rafey S. Balabanian (SBN – 315962)
rbalabanian@edelson.com
Lily E. Hough (SBN – 315277)
EDELSON PC
123 Townsend Street, Suite 100
San Francisco, California 94107
Tel: 415.234.5342
Fax: 415.373.9495

Shawn A. Williams (SBN – 213113)
shawnw@rgrdlaw.com
David W. Hall (SBN – 274921)
dhall@rgrdlaw.com
ROBBINS GELLER RUDMAN & DOWD LLP
Post Montgomery Center
One Montgomery Street, Suite 1800
San Francisco, California 94104
Tel: 415.288.4545
Fax: 415.288.4534

Paul J. Geller (Admitted *pro hac vice*)
pgeller@rgrdlaw.com
Stuart A. Davidson (Admitted *pro hac vice*)
sdavidson@rgrdlaw.com
Mark Dearman (Admitted *pro hac vice*)
mdearman@rgrdlaw.com
Christopher C. Martins (Admitted *pro hac vice*)
cmartins@rgrdlaw.com
ROBBINS GELLER RUDMAN & DOWD LLP
120 East Palmetto Park Road, Suite 500
Boca Raton, Florida 33432
Tel: 561.750.3000
Fax: 561.750.3364

Frank A. Richter (Admitted *pro hac vice*)

frichter@rgrdlaw.com
James E. Barz (Admitted *pro hac vice*)
jbarz@rgrdlaw.com
ROBBINS GELLER RUDMAN & DOWD LLP
200 S. Wacker, 31st Floor
Chicago, Illinois 60606
Tel: 312-674.4674

Travis E. Downs III (Admitted *pro hac vice*)
travisd@rgrdlaw.com
ROBBINS GELLER RUDMAN & DOWD LLP
655 West Broadway, Suite 1900
San Diego, California 92101
Tel: 619.231.1058
Fax: 619.231.7423

Joel H. Bernstein (Admitted *pro hac vice*)
jbernstein@labaton.com
Corban S. Rhodes (Admitted *pro hac vice*)
crhodes@labaton.com
Ross M. Kamhi (Admitted *pro hac vice*)
rkamhi@labaton.com
LABATON SUCHAROW LLP
140 Broadway
New York, New York 10005
Tel: 212.907.0700
Fax: 212.818.0477

Counsel for In re Facebook Biometric Info. Plaintiffs and the Putative Class