APPENDIX

APPENDIX A

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

NIMESH PATEL, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED; ADAM PEZEN; CARLO LICATA,
Plaintiffs-Appellees,
v.
FACEBOOK, INC.,
Defendant-Appellant.

No. 18-15982

D.C. No. 3:15-cv-03747-JD

OPINION

Appeal from the United States District Court
for the Northern District of California
James Donato, District Judge, Presiding

Argued and Submitted June 12, 2019
San Francisco, California

Filed August 8, 2019

Before: Ronald M. Gould and Sandra S. Ikuta, Circuit Judges, and Benita Y. Pearson,[*] District Judge.

Opinion by Judge Ikuta

SUMMARY[**]

Standing / Class Certification / Illinois Law

The panel affirmed the district court's order certifying a class under Fed. R. Civ. P. 23 of users of Facebook, Inc., who alleged that Facebook's facial-recognition technology violated Illinois's Biometric Information Privacy Act ("BIPA").

The panel held that plaintiffs alleged a concrete and particularized harm, sufficient to confer Article III standing, because BIPA protected the plaintiffs' concrete privacy interest, and violations of the procedures in BIPA actually harmed or posed a material risk of harm to those privacy interests. Specifically, the panel concluded that the development of a face template using facial-recognition technology without consent (as alleged in this case) invades an individual's private affairs and concrete interests.

---

[*] The Honorable Benita Y. Pearson, United States District Judge for the Northern District of Ohio, sitting by designation.

[**] This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

The panel held that the district court did not abuse its discretion in certifying the class. Specifically, the panel rejected Facebook's argument that Illinois's extraterritoriality doctrine precluded the district court from finding predominance. The panel further held that the district court did not abuse its discretion in determining that a class action was superior to individual actions in this case.

COUNSEL

Lauren R. Goldman (argued), Andrew J. Pincus, and Michael Rayfield, Mayer Brown LLP, New York, New York, for Defendant-Appellant.

John Aaron Lawson (argued) and Rafey S. Balabanian, Edelson PC, San Francisco, California; Susan K. Alexander and Shawn A. Williams, Robbins Geller Rudman & Dowd LLP, San Francisco, California; Michael P. Canty and Corban S. Rhodes, Labaton Sucharow LLP, New York, New York; for Plaintiffs-Appellees.

Susan Fahringer and Nicola Menaldo, Perkins Coie LLP, Seattle, Washington; Neal Kumar Katyal, Hogan Lovells US LLP, Washington, D.C.; Lauren Ruben, Perkins Coie LLP, Denver, Colorado; Thomas P. Schmidt, Hogan Lovells US LLP, New York, New York; Sara Solow, Hogan Lovells US LLP, Philadelphia, Pennsylvania; for Amicus Curiae Internet Association.

Nathan Freed Wessler, American Civil Liberties Union, New York, New York; Rebecca K. Glenberg, Roger Baldwin Foundation of ACLU, Chicago,

Illinois; Jacob A. Snow, American Civil Liberties Union Foundation of Northern California, San Francisco, California; Jennifer Lynch and Adam Schwartz, Electronic Frontier Foundation, San Francisco, California; Joseph Jerome, Center for Democracy & Technology, Washington, D.C.; Michael C. Landis, Illinois PIRG Education Fund Inc., Chicago, Illinois; for Amici Curiae American Civil Liberties Union, American Civil Liberties Union of Illinois, American Civil Liberties Union Foundation of Northern California, American Civil Liberties Union Foundation of Southern California, Center for Democracy & Technology, Electronic Frontier Foundation, and Illinois PIRG Education Fund Inc.

Marc Rotenberg, Alan Butler, and John Davisson, Electronic Privacy Information Center, Washington, D.C., for Amicus Curiae Electronic Privacy Information Center (EPIC).

Kelly P. Dunbar, Reginald J. Brown, Patrick J. Carome, Jonathan G. Cedarbaum, and Samuel M. Strongin, Wilmer Cutler Pickering Hale and Dorr LLP, Washington, D.C.; Steven P. Lehotsky and Jonathan D. Urick, U.S. Chamber Litigation Center, Washington, D.C.; for Amicus Curiae Chamber of Commerce of the United States of America.

OPINION

IKUTA, Circuit Judge:

Plaintiffs' complaint alleges that Facebook subjected them to facial-recognition technology without complying with an Illinois statute intended

to safeguard their privacy. Because a violation of the Illinois statute injures an individual's concrete right to privacy, we reject Facebook's claim that the plaintiffs have failed to allege a concrete injury-in-fact for purposes of Article III standing. Additionally, we conclude that the district court did not abuse its discretion in certifying the class.

I

Facebook operates one of the largest social media platforms in the world, with over one billion active users. *Packingham v. North Carolina*, 137 S. Ct. 1730, 1735 (2017). About seven in ten adults in the United States use Facebook.[1]

A

When a new user registers for a Facebook account, the user must create a profile and agree to Facebook's terms and conditions, which permit Facebook to collect and use data in accordance with Facebook's policies. To interact with other users on the platform, a Facebook user identifies another user as a friend and sends a friend request. If the request is accepted, the two users are able to share content, such as text and photographs.

For years, Facebook has allowed users to tag their Facebook friends in photos posted to Facebook. A tag identifies the friend in the photo by name and

---

[1] *See* John Gramlich, *10 Facts about Americans and Facebook*, Pew Research Ctr. (May 16, 2019), https://www.pewresearch.org/fact-tank/2019/05/16/facts-about-americans-and-facebook/.

includes a link to that friend's Facebook profile. Users who are tagged are notified of the tag, granted access to the photo, and allowed to share the photo with other friends or "un-tag" themselves if they choose.

In 2010, Facebook launched a feature called Tag Suggestions. If Tag Suggestions is enabled, Facebook may use facial-recognition technology to analyze whether the user's Facebook friends are in photos uploaded by that user. When a photo is uploaded, the technology scans the photo and detects whether it contains images of faces. If so, the technology extracts the various geometric data points that make a face unique, such as the distance between the eyes, nose, and ears, to create a face signature or map. The technology then compares the face signature to faces in Facebook's database of user face templates (i.e., face signatures that have already been matched to the user's profiles).[2] If there is a match between the face signature and the face template, Facebook may suggest tagging the person in the photo.

Facebook's face templates are stored on its servers, which are located in nine data centers maintained by Facebook. The six data centers located in the United States are in Oregon, California, Iowa, Texas, Virginia, and North Carolina. Facebook's headquarters are in California.

---

[2] According to Facebook, it creates and stores a template for a user when the user (1) has been tagged in at least one photo; (2) has not opted out of Tag Suggestions; and (3) satisfies other privacy-based and regulatory criteria.

B

Facebook users living in Illinois brought a class action against Facebook, claiming that Facebook's facial-recognition technology violates Illinois law. Class representatives Adam Pezen, Carlo Licata, and Nimesh Patel each live in Illinois. They joined Facebook in 2005, 2009, and 2008, respectively, and each uploaded photos to Facebook while in Illinois. Facebook created and stored face templates for each of the plaintiffs.

The three named plaintiffs filed the operative consolidated complaint in a California district court in August 2015. The plaintiffs allege that Facebook violated the Illinois Biometric Information Privacy Act (BIPA), 740 Ill. Comp. Stat. 14/1 *et seq*. (2008), which provides that "[a]ny person aggrieved" by a violation of its provisions "shall have a right of action" against an "offending party," *id.* 14/20. According to the complaint, Facebook violated sections 15(a) and 15(b) of BIPA by collecting, using, and storing biometric identifiers (a "scan" of "face geometry," *id.* 14/10) from their photos without obtaining a written release and without establishing a compliant retention schedule.[3]

---

[3] Sections 15(a) and (b) of BIPA provide:

> (a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or

The Illinois General Assembly enacted BIPA in 2008 to enhance Illinois's "limited State law

---

> obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.
>
> (b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> > (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
> >
> > (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
> >
> > (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

740 Ill. Comp. Stat. 14/15 (a)–(b).

regulating the collection, use, safeguarding, and storage of biometrics." 740 Ill. Comp. Stat. 14/5(e). BIPA defines a "biometric identifier" as including a "scan of hand or face geometry." *Id.* 14/10.[4] In a series of findings, the state legislature provided its views about the costs and benefits of biometric data use. The legislature stated that "[t]he use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings," and also noted that "[m]ajor national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions." *Id.* 14/5(a)–(b). Nevertheless, "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information," because while social security numbers can be changed if compromised by hackers, biometric data are "biologically unique to the individual," and "once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.* 14/5(c). Moreover, "[t]he full ramifications of biometric technology are not fully known." *Id.* 14/5(f). The legislature concluded that "[t]he public welfare,

---

[4] Section 10 of BIPA defines "biometric identifier" to mean "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 Ill. Comp. Stat. 14/10. Biometric identifiers do not include "writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color." *Id.*

security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." *Id.* 14/5(g).

To further these goals, section 15 of BIPA imposes "various obligations regarding the collection, retention, disclosure, and destruction of biometric identifiers and biometric information" on private entities. *Rosenbach v. Six Flags Entm't Corp.*, — N.E.3d —, 2019 IL 123186, at *4 (Ill. 2019). These requirements include "establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information" the earlier of three years after the individual's last interaction with the private entity or "when the initial purpose for collecting or obtaining such identifiers or information has been satisfied." 740 Ill. Comp. Stat. 14/15(a). The statute also requires the private entity to notify the individual in writing and secure a written release before obtaining a biometric identifier. *Id.* 14/15(b). BIPA also provides for actual and liquidated damages for violations of the Act's requirements. *Id.* 14/20.

C

In June 2016, Facebook moved to dismiss the plaintiffs' complaint for lack of Article III standing on the ground that the plaintiffs had not alleged any concrete injury. While Facebook's motion to dismiss was pending, the plaintiffs moved to certify a class under Rule 23 of the Federal Rules of Civil Procedure. The district court denied Facebook's motion to dismiss, and certified a Rule 23(b)(3) class

of "Facebook users located in Illinois for whom Facebook created and stored a face template after June 7, 2011." Facebook filed a timely petition for leave to appeal the district court's ruling under Rule 23(f). Fed. R. Civ. P. 23(f) (providing that "[a] court of appeals may permit an appeal from an order granting or denying class-action certification under this rule").

We have jurisdiction to review the district court's order granting class certification under 28 U.S.C. § 1292(e) and Rule 23(f) of the Federal Rules of Civil Procedure. We review de novo whether the plaintiffs have Article III standing. *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1024 (9th Cir. 2018), *as amended* (Apr. 20, 2018). The party invoking federal jurisdiction bears the burden of establishing the elements of Article III jurisdiction. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992). "At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice," and we "presume that general allegations embrace those specific facts that are necessary to support the claim." *Id.* (quotation and alteration omitted).

II

To establish Article III standing, a plaintiff "must have suffered an 'injury in fact'—an invasion of a legally protected interest which is (a) concrete and particularized; and (b) actual or imminent, not conjectural or hypothetical." *Id.* at 560 (cleaned up). A plaintiff does not necessarily meet the concrete injury requirement "whenever a statute grants a person a statutory right and purports to authorize

that person to sue to vindicate that right." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016), *as revised* (May 24, 2016) (*Spokeo I*). In other words, for Article III purposes, it is not enough for a plaintiff to allege that a defendant has violated a right created by a statute; we must still ascertain whether the plaintiff suffered a concrete injury-in-fact due to the violation.

A concrete injury need not be tangible. "Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete." *Id.* In determining whether an intangible injury is sufficiently concrete, we consider both history and legislative judgment. *Id.* We consider history because "it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Id.* We must also examine legislative judgment because legislatures are "well positioned to identify intangible harms that meet minimum Article III requirements." *Id.*

The Supreme Court has provided some guidance for determining whether a plaintiff has suffered a concrete injury due to a defendant's failure to comply with a statutory requirement. The violation of a statutory right that protects against "the risk of real harm" may be sufficient to constitute injury-in-fact, and under those circumstances a plaintiff "need not allege any *additional* harm beyond the one Congress has identified." *Id.* (emphasis in original). But a violation of a statutory procedural requirement that

does not present a material risk of harm, such as dissemination of "an incorrect zip code," likely does not cause a concrete injury. *Id.* at 1550.

In light of this guidance, we have adopted a two-step approach to determine whether the violation of a statute causes a concrete injury. We ask "(1) whether the statutory provisions at issue were established to protect [the plaintiff's] 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." *Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1113 (9th Cir. 2017) (*Spokeo II*).

Other cases demonstrate these principles. In *Van Patten v. Vertical Fitness Group, LLC*, for instance, we considered a Telephone Consumer Protection Act (TCPA) requirement prohibiting a telemarketer from calling or texting a consumer without the consumer's consent. 847 F.3d 1037, 1041–43 (9th Cir. 2017). The plaintiff alleged that a telemarketer violated this prohibition. *Id.* at 1041. We held that the TCPA was established to protect the plaintiff's substantive right to privacy, namely the right to be free from unsolicited telemarketing phone calls or text messages that "invade the privacy and disturb the solitude of their recipients." *Id.* at 1043. Because the telemarketer's conduct impacted this privacy right, we concluded that the plaintiff did not need to allege any additional harm beyond the one Congress identified, and therefore had alleged a concrete injury-in-fact sufficient to confer Article III standing. *Id.*

By contrast, in *Bassett v. ABM Parking Services, Inc.*, we considered a Fair Credit Reporting Act (FCRA) requirement that businesses redact certain credit card information, including the card's expiration date, on printed receipts. 883 F.3d 776, 777–78 (9th Cir. 2018). The plaintiff alleged that a parking garage had violated this requirement by giving him a receipt displaying his card's full expiration date. *Id.* at 778. We held that even if the FCRA created a substantive right to the "nondisclosure of a consumer's private financial information to identity thieves," the parking garage's failure to redact the credit card's expiration date did not impact this substantive right, because no one but the plaintiff himself saw the expiration date. *Id.* at 782–83. We therefore concluded that the plaintiff had failed to allege a concrete injury-in-fact. *Id.* at 783.

We apply our two-step approach to this case.

A

Facebook argues that the plaintiffs' complaint describes a bare procedural violation of BIPA rather than injury to a concrete interest, and therefore plaintiffs failed to allege that they suffered an injury-in-fact that is sufficiently concrete for purposes of standing.[5] Plaintiffs, in turn, argue that Facebook's violation of statutory requirements amounted to a violation of their substantive privacy rights, and so

[5] Facebook does not argue that the plaintiffs' alleged injury-in-fact is insufficiently particularized.

they suffered a concrete injury for purposes of Article III standing.

In addressing these arguments, we first consider "whether the statutory provisions at issue were established to protect [the plaintiff's] concrete interests (as opposed to purely procedural rights)." *Dutta v. State Farm Mut. Auto. Ins. Co.*, 895 F.3d 1166, 1174 (9th Cir. 2018) (alteration in original) (quoting *Spokeo II*, 867 F.3d at 1113). Privacy rights have long been regarded "as providing a basis for a lawsuit in English or American courts." *Spokeo I*, 136 S. Ct. at 1549. The common law roots of the right to privacy were first articulated in the 1890s in an influential law review article that reviewed 150 years of privacy-related case law and identified "a general right to privacy" in various common law property and defamation actions. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 198 (1890). Courts subsequently recognized that a distinct right to privacy existed at common law, *see, e.g.*, *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68, 69–71 (Ga. 1905), and treatises later identified four privacy torts recognized at common law, including "unreasonable intrusion upon the seclusion of another,"[6] Restatement (Second) of

[6] The Restatement (Second) of Torts § 652A(2) (1977) provides:

> The right of privacy is invaded by
>
> > (a) unreasonable intrusion upon the seclusion of another, as stated in § 652B; or

Torts § 652A. Soon, "the existence of a right of privacy [was] recognized in the great majority of the American jurisdictions that have considered the question." Restatement (Second) of Torts § 652A cmt. a.

The Supreme Court has likewise recognized the common law roots of the right to privacy. *See U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 & n. 15 (1989) (recognizing the common law's protection of a privacy right); *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469, 488 (1975) (noting that a right of privacy had been recognized at common law in the majority of American jurisdictions). We have also recognized the common law roots of the right to privacy. *See Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017) ("Violations of the right to privacy have long been actionable at common law."); *Van Patten*, 847 F.3d at 1043 ("Actions 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.") (citing Restatement (Second) of Torts § 652B).

(b) appropriation of the other's name or likeness, as stated in § 652C; or

(c) unreasonable publicity given to the other's private life, as stated in § 652D; or

(d) publicity that unreasonably places the other in a false light before the public, as stated in § 652E.

These common law privacy rights are intertwined with constitutionally protected zones of privacy. *See Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 569 n.7 (1963) (Douglas, J., concurring) ("A part of the philosophical basis of [the First Amendment right to privacy] has its roots in the common law."); *see also Kyllo v. United States*, 533 U.S. 27, 34 (2001) ("[I]n the case of the search of the interior of homes—the prototypical and hence most commonly litigated area of protected privacy—there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*." (emphasis in original)). As one commentator summed up, "[d]espite the differences between tort law and constitutional protections of privacy, it is still reasonable to view the interests and values that each protect as connected and related." Eli A. Meltz, Note, *No Harm, No Foul? "Attempted" Invasion of Privacy and the Tort of Intrusion Upon Seclusion*, 83 Fordham L. Rev. 3431, 3437 (2015).

In its recent Fourth Amendment jurisprudence, the Supreme Court has recognized that advances in technology can increase the potential for unreasonable intrusions into personal privacy. These concerns extend to sense-enhancing thermal imaging, *see Kyllo*, 533 U.S. at 34; GPS monitoring for extended periods of time, *see United States v. Jones*, 565 U.S. 400, 416, 428 (2012) (Sotomayor, J., concurring, and Alito, J., concurring) (five justices agreeing that privacy concerns are raised by such monitoring, as later recognized in *Carpenter v. United States*, 138 S. Ct. 2206, 2215 (2018)); modern

cell phone storage of "vast quantities of personal information," *Riley v. California*, 573 U.S. 373, 386 (2014); and technological advances in tracking cell-site location information, *see Carpenter*, 138 S. Ct. at 2215. Technological advances provide "access to a category of information otherwise unknowable," *id.* at 2218, and "implicate privacy concerns" in a manner as different from traditional intrusions as "a ride on horseback" is different from "a flight to the moon," *Riley*, 573 U.S. at 393.

In light of this historical background and the Supreme Court's views regarding enhanced technological intrusions on the right to privacy, we conclude that an invasion of an individual's biometric privacy rights "has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Spokeo I*, 136 S. Ct. at 1549. "[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person." *Reporters Comm.*, 489 U.S. at 763. As in the Fourth Amendment context, the facial-recognition technology at issue here can obtain information that is "detailed, encyclopedic, and effortlessly compiled," which would be almost impossible without such technology. *Carpenter*, 138 S. Ct. at 2216. Once a face template of an individual is created, Facebook can use it to identify that individual in any of the other hundreds of millions of photos uploaded to Facebook each day, as well as determine when the individual was present at a specific location. Facebook can also identify the individual's Facebook friends or acquaintances who

are present in the photo. Taking into account the future development of such technology as suggested in *Carpenter*, *see* 138 S. Ct. at 2216, it seems likely that a face-mapped individual could be identified from a surveillance photo taken on the streets or in an office building. Or a biometric face template could be used to unlock the face recognition lock on that individual's cell phone. We conclude that the development of a face template using facial-recognition technology without consent (as alleged here) invades an individual's private affairs and concrete interests. Similar conduct is actionable at common law.

The judgment of the Illinois General Assembly, which is "instructive and important" to our standing inquiry, *Spokeo II*, 867 F.3d at 1112 (quotation omitted), supports the conclusion that the capture and use of a person's biometric information invades concrete interests. As noted above, in enacting BIPA, the General Assembly found that the development and use of biometric data presented risks to Illinois's citizens, and that "[t]he public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 Ill. Comp. Stat. 14/5(g). Interpreting the statute, the Illinois Supreme Court concluded that "[t]he strategy adopted by the General Assembly through enactment of [BIPA]" was to protect individuals' "biometric privacy" by (1) "imposing safeguards to insure that individuals' and customers' privacy rights in their biometric identifiers and biometric information are properly honored and protected to

begin with, before they are or can be compromised," and (2) "by subjecting private entities who fail to follow the statute's requirements to substantial potential liability." *Rosenbach*, 2019 IL 123186, at *6–7. Based on this interpretation, the Illinois Supreme Court concluded that an individual could be "aggrieved" by a violation of BIPA whenever "a private entity fails to comply with one of section 15's requirements," because "that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach." *Id.* at *6. Individuals are not required to sustain a "compensable injury beyond violation of their statutory rights before they may seek recourse." *Id.* at *7.

Therefore, we conclude that "the statutory provisions at issue" in BIPA were established to protect an individual's "concrete interests" in privacy, not merely procedural rights. *Spokeo II*, 867 F.3d at 1113.

B

We next turn to the question "whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests." *Spokeo II*, 867 F.3d at 1113. Facebook's relevant conduct, according to the complaint, is the collection, use, and storage of biometric identifiers without a written release, in violation of section 15(b), and the failure to maintain a retention schedule or guidelines for destroying biometric identifiers, in violation of section 15(a). The plaintiffs

allege that a violation of these requirements allows Facebook to create and use a face template and to retain this template for all time. Because the privacy right protected by BIPA is the right not to be subject to the collection and use of such biometric data, Facebook's alleged violation of these statutory requirements would necessarily violate the plaintiffs' substantive privacy interests. As the Illinois Supreme Court explained, the procedural protections in BIPA "are particularly crucial in our digital world" because "[w]hen a private entity fails to adhere to the statutory procedures . . . the right of the individual to maintain his or her biometric privacy vanishes into thin air." *Rosenbach*, 2019 IL 123186, at *6 (cleaned up). Accordingly, we conclude that the plaintiffs have alleged a concrete injury-in-fact sufficient to confer Article III standing.

We reached a similar conclusion in *Eichenberger*, which considered whether a plaintiff had standing to bring a complaint alleging a violation of the Video Privacy Protection Act, which barred a videotape provider from knowingly disclosing "personally identifiable information concerning any consumer of such provider." 876 F.3d at 983 (quoting 18 U.S.C. § 2710(b)(1)). We concluded that the plaintiff had Article III standing because every unlawful disclosure of an individual's personally identifiable information and video-viewing history offended the individual's "substantive privacy interest in his or her video-viewing history." *Id.* Under the common law, an intrusion into privacy rights by itself makes a defendant subject to liability. *See* Restatement (Second) of Torts § 652B. In other words, "privacy

torts do not always require additional consequences to be actionable." *Eichenberger*, 876 F.3d at 983 (citing Restatement (Second) of Torts § 652B cmt. b); *see also Van Patten*, 847 F.3d at 1043.

Given the nature of the alleged violation of BIPA, Facebook's reliance on *Bassett v. ABM Parking Services, Inc.*, 883 F.3d at 780, is misplaced. Although the parking service in that case technically violated the FCRA by failing to redact a credit card's expiration date, that violation did not cause a disclosure of the consumer's private financial information, the substantive harm the FCRA was designed to vindicate. *Id.* at 782–83. By contrast, Facebook's alleged collection, use, and storage of plaintiffs' face templates here is the very substantive harm targeted by BIPA. Because we conclude that BIPA protects the plaintiffs' concrete privacy interests and violations of the procedures in BIPA actually harm or pose a material risk of harm to those privacy interests, *see Dutta*, 895 F.3d at 1174, the plaintiffs have alleged a concrete and particularized harm, sufficient to confer Article III standing.

III

We now turn to Facebook's argument that the district court abused its discretion by certifying the class. We review a district court's order granting class certification for abuse of discretion, *Sali v. Corona Reg'l Med. Ctr.*, 909 F.3d 996, 1002 (9th Cir. 2018), *as amended* (Nov. 27, 2018), but give the district court "noticeably more deference when reviewing a grant of class certification than when

reviewing a denial," *Just Film, Inc. v. Buono*, 847 F.3d 1108, 1115 (9th Cir. 2017) (quotation omitted). An error of law is "a per se abuse of discretion." *Sali*, 909 F.3d at 1002 (quotation omitted). We review the district court's findings of fact for clear error, and its legal conclusions de novo. *See id.*

First, Facebook urges that class certification is not compatible with Rule 23(b)(3) of the Federal Rules of Civil Procedure, which requires that "questions of law or fact common to class members predominate over any questions affecting only individual members." Fed. R. Civ. P. 23(b)(3). According to Facebook, the Illinois extraterritoriality doctrine precludes the district court from finding predominance.

The Illinois Supreme Court has held that it is a "longstanding rule of construction in Illinois" that "a 'statute is without extraterritorial effect unless a clear intent in this respect appears from the express provisions of the statute.'" *Avery v. State Farm Mut. Auto. Ins. Co.*, 835 N.E.2d 801, 852 (Ill. 2005) (quoting *Dur-Ite Co. v. Indus. Comm'n*, 68 N.E.2d 717, 722 (Ill. 1946)). In the absence of such an intent, an Illinois plaintiff may not maintain a cause of action under a state statute for transactions that took place outside of Illinois. *Id.* at 853. When a case is "made up of components that occur in more than one state," plaintiffs may maintain an action only if the events that are necessary elements of the transaction occurred "primarily and substantially within" Illinois. *Id.* at 853–54.

Facebook insists that the Illinois legislature did not intend for the BIPA to have extraterritorial effect, and in the absence of such an intent, a court would have to consider whether the relevant events at issue took place inside or outside Illinois. Facebook argues that its collection of biometric data and creation of a face template occurred on its servers outside of Illinois, and therefore the necessary elements of any violation occurred extraterritorially. At best, Facebook argues, each class member would have to provide individualized proof that events in that class member's case occurred "primarily and substantially within" Illinois; for instance, that the member was in Illinois when the scanned photo was taken or uploaded, when a facial recognition analysis was performed, when the photo was tagged or given a tag suggestion, or for similar events. Because the district court would have to conduct countless mini-trials to determine whether the events in each plaintiff's case occurred "primarily and substantially within" Illinois, Facebook posits, common questions do not predominate, and the district court erred in certifying the class.

We disagree. The parties' dispute regarding extraterritoriality requires a decision as to where the essential elements of a BIPA violation take place. The statute does not clarify whether a private entity's collection, use, and storage of face templates without first obtaining a release, or a private entity's failure to implement a compliant retention policy, is deemed to occur where the person whose privacy rights are impacted uses Facebook, where Facebook scans photographs and stores the face templates, or

in some other place or combination of places. Given the General Assembly's finding that "[m]ajor national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions," 740 Ill. Comp. Stat. 14/5, it is reasonable to infer that the General Assembly contemplated BIPA's application to individuals who are located in Illinois, even if some relevant activities occur outside the state. These threshold questions of BIPA's applicability can be decided on a class-wide basis. If the violation of BIPA occurred when the plaintiffs used Facebook in Illinois, then the relevant events occurred "primarily and substantially" in Illinois, and there is no need to have mini-trials on this issue.[7] If the violation of BIPA occurred when Facebook's servers created a face template, the district court can determine whether Illinois's extraterritoriality doctrine precludes the application of BIPA. In either case, predominance is not defeated. And of course, if future decisions or circumstances lead to the conclusion that extraterritoriality must be evaluated on an individual basis, the district court can decertify the class. *See Officers for Justice v. Civil Serv. Comm'n*, 688 F.2d 615, 633 (9th Cir.1982) ("[A] district court's order respecting class status is not final or irrevocable, but rather, it is inherently tentative."); *see also* Fed. R. Civ. P. 23(c)(1)(C) ("An

[7] The district court found that this case involves only plaintiffs who are located in Illinois, and the claims are based on the application of Illinois law to the use of Facebook mainly in Illinois.

order that grants or denies class certification may be altered or amended before final judgment.").

Second, Facebook argues that the district court abused its discretion by certifying the class because a class action is not superior to individual actions. "Rule 23(b)(3) requires that a class action be 'superior to other available methods for fairly and efficiently adjudicating the controversy,' and it specifically mandates that courts consider 'the likely difficulties in managing a class action.'" *Briseno v. ConAgra Foods, Inc.*, 844 F.3d 1121, 1127–28 (9th Cir. 2017) (quoting Fed. R. Civ. P. 23(b)(3)(D)). According to Facebook, the possibility of a large, class-wide statutory damages award here defeats superiority.

We disagree. The question "whether the potential for enormous liability can justify a denial of class certification depends on [legislative] intent." *Bateman v. Am. Multi-Cinema, Inc.*, 623 F.3d 708, 722 (9th Cir. 2010). Where neither the statutory language nor legislative history indicates that the legislature intended to place a cap on statutory damages, denying class certification on that basis would "subvert [legislative] intent." *Id.* at 722–23; *cf. Kline v. Coldwell, Banker & Co.*, 508 F.2d 226, 228, 235 (9th Cir. 1974) (holding that a potential liability of $750 million under the Sherman Act would be inconsistent with congressional intent in enacting the statutory damages provision because treble damages were "not remedial" but "punitive"). Here, nothing in the text or legislative history of BIPA indicates that a large statutory damages award would be contrary to the intent of the General

Assembly. Therefore, the district court did not abuse its discretion in determining that a class action is superior to individual actions in this case. *See* Fed. R. Civ. P. 23(b)(3).[8]

AFFIRMED.

[8] In its brief on appeal, Facebook also argued that only a "person aggrieved" by a BIPA violation could bring a private cause of action, and therefore the plaintiff must allege some harm beyond a violation of the statute itself. Facebook claimed that because each plaintiff must allege such individualized harms, predominance under Rule 23 of the Federal Rules of Civil Procedure was defeated. Because Facebook's interpretation of BIPA was rejected by the Illinois Supreme Court, *see Rosenbach*, 2019 IL 123186, at *4, which was decided after the briefing in this case, this argument is foreclosed.

APPENDIX B

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

NIMESH PATEL, ET AL.,

Plaintiffs,

v.

FACEBOOK INC.,

Defendant.

Case No. 3:15-cv-03747-JD

ORDER RE RENEWED MOTION TO DISMISS FOR LACK OF SUBJECT MATTER JURISDICTION

Re: Dkt. No. 227

Filed: 02/26/2018

In this putative class action case under the Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1 *et seq*. ("BIPA"), named plaintiffs allege that defendant Facebook, Inc. ("Facebook") unlawfully collected and stored their biometric data without prior notice or consent. Dkt. No. 40. Facebook asks to dismiss the case under Federal Rule of Civil Procedure 12(b)(1) and *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) *(Spokeo I)* on the

ground that plaintiffs have failed to allege a concrete injury in fact. Dkt. No. 227. The motion is denied.

BACKGROUND

This consolidated action originated as three separate cases originally filed in Illinois courts. Two of the cases were filed in federal court, while a third was filed in Illinois state court and removed to federal court by Facebook under the Class Action Fairness Act. Notice of Removal, Licata v. Facebook, Inc., No. 1:15-cv-04022 (N.D. Ill. filed May 6, 2015) (No. 1). The parties stipulated to transfer the cases to this Court, where they were consolidated into a single action. *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1159 (2016). The consolidated class action complaint, Dkt. No. 40, is the operative complaint.

The consolidated complaint alleges that Facebook "operates the largest social network in the world, with over one billion active users." Dkt. No. 40 ¶ 1. The named plaintiffs, Nimesh Patel, Adam Pezen and Carlo Licata, use Facebook "to, among other things, upload and share photographs with friends and relatives." *Id.* ¶¶ 2, 7-9.

Plaintiffs' claims arise out of Facebook's "Tag Suggestions" program launched in 2010. *Id.* ¶ 3. A user "tags" other Facebook users and non-users by identifying them in photographs uploaded to Facebook. *Id.* ¶ 2. "Tag Suggestions" is intended to encourage more tagging. *Id.* ¶ 3. It scans uploaded photographs "and then identif[ies] faces appearing in those photographs." *Id.* If the program "recognizes and identifies one of the faces appearing in [a]

photograph, Facebook will suggest that individual's name or automatically tag them." *Id.* In effect, the program associates names with faces in photos and prompts users to tag those people.

Tag Suggestions uses "state-of-the-art facial recognition technology" to extract biometric identifiers from photographs that users upload. *Id.* ¶¶ 4, 22. Facebook creates and stores digital representations (known as "templates") of people's faces based on the geometric relationship of facial features unique to each individual, "like the distance between [a person's] eyes, nose and ears." *Id.* ¶ 23.

Plaintiffs allege that Facebook collected users' biometric data secretly and without consent. Specifically, they allege that the Tag Suggestions program violated BIPA because Facebook did not: "[1] properly inform plaintiffs or the class in writing that their biometric identifiers (face geometry) were being generated, collected or stored; [2] properly inform plaintiffs or the class in writing of the specific purpose and length of time for which their biometric identifiers were being collected, stored, and used; [3] provide a publicly available retention schedule and guidelines for permanently destroying the biometric identifiers of plaintiffs and the class (who do not opt-out of 'Tag Suggestions'); and [4] receive a written release from plaintiffs or the class to collect, capture, or otherwise obtain their biometric identifiers." *Id.* ¶ 5. Plaintiffs seek declaratory and injunctive relief and statutory damages. *Id.* ¶ 6.

DISCUSSION

I. Legal Standards

"A Rule 12(b)(1) jurisdictional attack may be facial or factual. In a facial attack, the challenger asserts that the allegations contained in a complaint are insufficient on their face to invoke federal jurisdiction. By contrast, in a factual attack, the challenger disputes the truth of the allegations that, by themselves, would otherwise invoke federal jurisdiction." *Safe Air for Everyone v. Meyer,* 373 F.3d 1035, 1039 (9th Cir. 2004) (citations omitted).

In a facial jurisdictional challenge, the Court takes all factual allegations in the complaint as true and draws all reasonable inferences in plaintiffs' favor. *Pride v. Correa,* 719 F.3d 1130, 1133 (9th Cir. 2013). In a factual challenge, the Court "may review evidence beyond the complaint without converting the motion to dismiss into a motion for summary judgment" and "need not presume the truthfulness of the plaintiff's allegations." *Safe Air,* 373 F.3d at 1039 (citations omitted). This discretion should be used with caution so that it does not usurp a merits determination. A "jurisdictional finding of genuinely disputed facts is inappropriate when the jurisdictional issue and substantive issues are so intertwined that the question of jurisdiction is dependent on the resolution of factual issues going to the merits of an action." *Id.* (internal quotations and citations omitted).

II. Article III Standing

Federal courts are courts of limited jurisdiction, and the "case or controversy" requirement of Article

III of the U.S. Constitution "limits federal courts' subject matter jurisdiction by requiring, inter alia, that plaintiffs have standing." *Chandler v. State Farm Mut. Auto. Ins. Co.*, 598 F.3d 1115, 1121 (9th Cir. 2010). As the Supreme Court recently reiterated, a plaintiff must demonstrate standing to sue by alleging the "irreducible constitutional minimum" of (1) an "injury in fact" (2) that is "fairly traceable to the challenged conduct of the defendants" and (3) "likely to be redressed by a favorable judicial decision." *Spokeo I*, 136 S. Ct. at 1547. These requirements may not be abrogated by Congress. *Id.* at 1548. The specific element of injury in fact is satisfied when the plaintiff has "suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Id.* (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)).

Spokeo I did not announce new standing requirements, as the citation to *Lujan* indicates. Rather, it sharpened the focus on when an intangible harm such as the violation of a statutory right is sufficiently concrete to rise to the level of an injury in fact. To determine whether an injury in fact has been demonstrated in this "somewhat murky area," *Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1112 (9th Cir. 2017) *(Spokeo II),* the Supreme Court has held that "both history and the judgment of Congress play important roles." *Spokeo I*, 136 S. Ct. at 1549. History is instructive because an intangible harm is likely to be concrete for standing purposes when it bears "a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit." *Id.* Congress's judgment is particularly

important because it is "well positioned to identify intangible harms" that are in fact concrete for Article III purposes. *Id.* Congress has the power to create statutory rights and causes of action "that will give rise to a case or controversy where none existed before." *Id.* Consequently, an intangible harm such as "the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact. In other words, a plaintiff in such a case need not allege any additional harm beyond the one Congress has identified." *Id.*

While *Spokeo I* refers to Congress, neither side disputes that state legislatures are equally well-positioned to determine when an intangible harm is a concrete injury. Our circuit said as much when it held that "state law can create interests that support standing in federal courts. If that were not so, there would not be Article III standing in most diversity cases, including run-of-the-mill contract and property disputes. State statutes constitute state law that can create such interests." *Cantrell v. City of Long Beach*, 241 F.3d 674, 684 (9th Cir. 2001). While this conclusion pre-dates *Spokeo I,* nothing there undercuts it. To be sure, state law cannot create Article III standing where none exists under our federal precedents. But there is no good reason why the judgment of a state legislature should be treated as less important than that of Congress in deciding when the violation of a statutory grant in itself amounts to a real and concrete injury.

Our circuit has adopted decisions from sister circuits to hold that "an alleged procedural violation [of a statute] can by itself manifest concrete injury where Congress conferred the procedural right to

protect a plaintiff's concrete interests and where the procedural violation presents 'a real risk of harm' to that concrete interest." *Spokeo II,* 867 F.3d at 1113 (internal citations omitted) (brackets in original). The dispositive inquiries are whether: (1) the statutory provisions at issue were established to protect the plaintiff's concrete interests; and (2) the specifically alleged procedural violations "actually harm or present a material risk of harm" to those interests. *Id.*

III. Concrete Injury

The plain language of BIPA drives the standing analysis in this case. BIPA expresses the judgments of the Illinois legislature about the rights of Illinois citizens with respect to the collection of personal biometric data by corporations and businesses. *In re Facebook*, 185 F. Supp. 3d at 1169 (citing 740 Ill. Comp. Stat. 14/5(b)). Specifically, BIPA manifests the Illinois legislature's conclusions that:

(1) Biometrics are uniquely sensitive identifiers. "Biometrics are unlike other unique identifiers . . . [and] are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." 740 Ill. Comp. Stat. 14/5(c).

(2) Biometric technology is a new frontier subject to unpredictable developments. "The full ramifications of biometric technology are not fully known." *Id.* at 14/5(f).

(3) People are apprehensive of transactions involving their biometrics. The "overwhelming

majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information" and are "deterred from partaking in biometric identifier-facilitated transactions." *Id.* at 14/5(d)-(e).

(4) Regulation of biometric collection, use, and storage serves the public interest. The "public welfare, security and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." *Id.* at 14/5(g).

To address these concerns and protect the rights of its residents to control their biometric information, the Illinois legislature enacted several measures. Section 15(a) of BIPA requires private entities possessing biometric data to publish written policies on data retention and destruction. Section 15(b) provides that biometric data may not be obtained without (1) written notice that biometric data is at issue, (2) written notice of why and for how long the data is being collected and stored, and (3) written consent from the subject. Sections 15(c) and (d) limit the sale, trade, and disclosure of biometric data, and Section 15(e) sets security standards for storing data. Plaintiffs have sued under Sections 15(a) and (b) for lack of notice and consent.

These provisions, along with the plain text of BIPA as a whole, leave little question that the Illinois legislature codified a right of privacy in personal biometric information. There is equally little doubt about the legislature's judgment that a violation of BIPA's procedures would cause actual and concrete harm. BIPA vested in Illinois residents the right to

control their biometric information by requiring notice before collection and giving residents the power to say no by withholding consent. As the Illinois legislature found, these procedural protections are particularly crucial in our digital world because technology now permits the wholesale collection and storage of an individual's unique biometric identifiers -- identifiers that cannot be changed if compromised or misused. When an online service simply disregards the Illinois procedures, as Facebook is alleged to have done, the right of the individual to maintain her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized.

Consequently, the abrogation of the procedural rights mandated by BIPA necessarily amounts to a concrete injury. This injury is worlds away from the trivial harm of a mishandled zip code or credit card receipt. A violation of the BIPA notice and consent procedures infringes the very privacy rights the Illinois legislature sought to protect by enacting BIPA. That is quintessentially an intangible harm that constitutes a concrete injury in fact. *See Spokeo II*, 867 F.3d at 1113 (and cases cited therein).

The Illinois legislature's considered judgments in enacting BIPA are also well-grounded in a long tradition of claims actionable in privacy law. The "'common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person.'" *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017) (quoting *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989)). "Violations of the right to privacy have long

been actionable at common law." *Id.* "Actions 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 v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1043 (9th Cir. 2017) (citing Restatement (Second) of Torts § 652(B) (Am. Law Inst. 1977)).

Facebook insists that the collection of biometric information without notice or consent can never support Article III standing without "*real-world* harms" such as adverse employment impacts or even just "anxiety." *See, e.g.,* Dkt. No. 227 at 1, and 5-7 (emphasis in original). That contention exceeds the law. The Supreme Court has expressly recognized that the violation of statutory procedural rights in itself can be sufficient, without any additional harm alleged. *Spokeo I*, 136 S.Ct. at 1549. Our circuit has also found that "privacy torts do not always require additional consequences to be actionable." *Eichenberger*, 876 F.3d at 983. Intrusion on privacy alone can be a concrete injury. *Id.; see also Mount v. PulsePoint, Inc.*, 684 F. App'x 32, 34 (2d Cir. 2017), as amended (May 3, 2017) (unauthorized access to and monitoring of web-browsing is concrete injury); *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 843 (N.D. Cal. 2017) (tracking users' web-browsing history is concrete injury). Our circuit has specifically affirmed findings of concrete injury, and standing to sue, when plaintiffs were deprived of procedures that protected privacy interests without any attendant embarrassment, job loss, stress or other additional injury. *See, e.g., Syed v. M-I, LLC*, 853 F.3d 492, 499 (9th Cir. 2017) (loss of statutory

right to authorize credit check by prospective employer); *Eichenberger,* 876 F.3d at 983-84 (loss of control over personal information under Video Privacy Protection Act).

The cases Facebook relies upon to contest standing are readily distinguishable. In *Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909 (7th Cir. 2017), for example, the plaintiff sued Time Warner for retaining his social security number and other personal information in violation of the Cable Communications Policy Act. But that is of scant relevance here because BIPA expressly recognizes that social security numbers do not implicate the kinds of privacy concerns that biometric identifiers do. Biometric identifiers, as the Illinois legislature found, are "unlike other unique identifiers" such as "social security numbers," because those "when compromised, can be changed." 740 Ill. Comp. Stat. 14/5(c).

In *McCollough v. Smarte Carte, Inc.*, No. 16 C 03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016), a case brought under BIPA, locker rental customers in Illinois had to complete their rentals by "plac[ing] their finger on a fingerprint scanner, which is then displayed on the screen; finally, the screen displays the locker number and unlocks the locker." *Id.* at *1. The court found that "a customer would understand that Smarte Carte collects and retains their fingerprint data for at least the duration of the rental. The system would not work otherwise." *Id.* n.1.

So too for *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499, 513 (S.D.N.Y. 2017),

another decision under BIPA that the Second Circuit affirmed in part, vacated in part, and remanded in *Santana v. Take-Two Interactive Software, Inc.*, __ Fed. Appx. __, No. 17-303, 2017 WL 5592589 (2d Cir. Nov. 21, 2017). In that case, the plaintiffs bought a basketball videogame that allowed players to create personalized "avatars" using their own faces. 2017 WL 5592589 at *1. To make an avatar, players had to scan their faces for approximately 15 minutes by standing "within 6 to 12 inches of the camera" and slowly moving "their heads 30 degrees to the left and to the right." *Id.* Critically, before a player could create an avatar, she was required to consent by pressing "continue" after reading a notice stating that the "face scan" might be recorded. *Id.* In these circumstances, the district court found that the plaintiffs clearly knew that "Take-Two had to collect data based upon their faces in order to create the personalized basketball avatars, and that a derivative of the data would be stored in the resulting digital faces of those avatars so long as those avatars existed." *Vigil*, 235 F. Supp. 3d at 515. The Second Circuit had little troubling concluding that Take-Two had satisfied BIPA's notice and consent provisions, and that the plaintiffs could not allege a material risk of harm to a concrete interest protected by the statute. 2017 WL 5592589 at *3.

While *McCullough* and *Vigil* involved BIPA, they turned on circumstances that are a far cry from the ones alleged here. In those cases, the plaintiffs indisputably knew that their biometric data would be collected before they accepted the services offered by the businesses involved. *Vigil* had the specific fact of prior written notice and click-through consent. In

each case, the plaintiffs had sufficient notice to make a meaningful decision about whether to permit the data collection. That factual difference makes these cases of little value in addressing the allegations in the consolidated complaint that Facebook afforded plaintiffs no notice and no opportunity to say no.

Facebook's reliance on *Spokeo II* is also misplaced. It highlights a comment in a footnote that a plaintiff might have a hard time showing standing under FCRA provisions "which do *not* turn on any alleged reporting inaccuracy." *Spokeo II*, 867 F.3d at 1116 n.2 (emphasis in original). This point appears to be a further elaboration on Facebook's "real harm" contention and is unpersuasive for the same reasons. But even taken on its own, it is again of little relevance because BIPA, unlike FCRA, targets the unauthorized collection of information in the first instance. The two statutes are sufficiently distinct so that *Spokeo II's* FCRA concerns simply do not apply here. *See Eichenberger*, 876 F.3d at 983-84 *(Spokeo I* and *II* distinguishable because Video Privacy Protection Act, unlike FCRA, identifies a substantive right to privacy). In addition, as the footnote itself suggests, the comment is likely dicta because the plaintiff in *Spokeo II* did not allege a claim independent of a reporting inaccuracy. *Spokeo II*, 867 F.3d at 1116 n.2.

In addition to its legal arguments, Facebook has submitted its user agreement and data policy, deposition excerpts and other extrinsic evidence to contend that BIPA's notice and consent requirements were actually satisfied. *See, e.g.*, Dkt. No. 227 at 10-11. While that may or may not prove true in the end, the salient point for present purposes is that notice

and consent are inextricably intertwined with the merits of plaintiffs' claims. The parties contest the facts surrounding those issues, in contrast to the largely undisputed material facts in *McCullough* and *Vigil*. These dispositive disputes on the merits should be decided on summary judgment or at trial, and not in the Rule 12(b)(1) jurisdictional context. *Safe Air*, 373 F.3d at 1039.

CONCLUSION

Facebook's motion to dismiss for lack of subject matter jurisdiction is **DENIED.**

IT IS SO ORDERED.

Dated: February 26, 2018

/s/ James Donato
JAMES DONATO
United States District Judge

APPENDIX C

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

IN RE FACEBOOK BIOMETRIC INFORMATION PRIVACY LITIGATION

THIS DOCUMENT RELATES TO: ALL ACTIONS

Case No. 3:15-cv-03747-JD

ORDER RE CLASS CERTIFICATION

Re: Dkt. No. 255

Filed: 04/16/2018

In this privacy action against defendant Facebook, Inc. ("Facebook"), named plaintiffs Nimesh Patel, Adam Pezen, and Carlo Licata move for class certification. Dkt. No. 255. Plaintiffs' claims are sufficiently cohesive to allow for a fair and efficient resolution on a class basis. Consequently, the case will proceed with a class consisting of Facebook users located in Illinois for whom Facebook created and stored a face template after June 7, 2011.

BACKGROUND

The material facts of this case are reported in a number of prior orders. *See, e.g., Patel v. Facebook Inc.*, __ F. Supp. 3d. __, No. 3:15-cv-03747-JD, 2018

WL 1050154, at *1 (N.D. Cal. Feb. 26, 2018) ["*Spokeo* order"]. Briefly summarized, plaintiffs are Facebook users who challenge its "Tag Suggestions" program, which scans for and identifies people in uploaded photographs to promote user tagging. Plaintiffs allege that Facebook collects and stores their biometric data without prior notice or consent in violation of their privacy rights and Sections 15(a) and 15(b) of the Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1 *et seq*. ("BIPA"). Dkt. No. 40.

The salient facts for class certification are undisputed. Facebook launched Tag Suggestions on June 7, 2011. Dkt. No. 255 at 2. In broad strokes, Tag Suggestions is powered by a four-step facial recognition process. Initially, the software tries to detect faces (the "detection" step) and standardizes any detected faces for qualities like orientation and size (the "alignment step"). Dkt. No. 256-8 ¶¶ 13-17. For each face that is detected and aligned, Facebook computes a "face signature," which is a "string of numbers that represents a particular image of a face" (the "representation" step). *Id.* ¶ 18. Face signatures are then run through a stored database of user "face templates" to look for matches (the "classification" step). *Id.* ¶¶ 21-23. A face template is "a string of numbers that represents a boundary" between the face signatures of a given Facebook user and the face signatures of others, and is calculated based on that user's photographs. *Id.* If a computed face signature falls within the boundary described by a user's face template, Facebook suggests tagging the user. *See* Dkt. No. 284-20 at 37. Facebook represents, with no challenge from plaintiffs, that face

signatures are not stored. Dkt. No. 256-8 ¶ 20. Only face templates are kept by Facebook.

Facebook's facial recognition technology is reliable but not foolproof. Facebook estimates that 90% of faces appearing in photographs are successfully detected, and of those detected faces, 85% are successfully aligned. Dkt. No. 284-9 ¶¶ 5-6. That means approximately 76% of faces appearing in photographs reach the representation step and have face signatures computed. Facebook states that in 2014, it was able to match around 67% of detected faces with users, which somewhat understates current matches because the rate has risen as the technology has matured. *Id.* ¶¶ 8-9.

Plaintiffs seek certification under Federal Rule of Civil Procedure 23(b)(3) and propose a class of all "Facebook users living in Illinois whose face appeared in a photo uploaded to Facebook from Illinois between June 7, 2011, and the final disposition of this action." Dkt. No. 255 at 5. Plaintiffs also propose an alternative class of all "people living in Illinois for whom Facebook has a stored 'face template' that was created between June 7, 2011, and final disposition of this action." *Id.*

LEGAL STANDARDS

As the parties seeking certification, plaintiffs bear the burden of showing that the requirements of Federal Rule of Civil Procedure 23 are met. *Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 588 (9th Cir. 2012). The proposed class action must satisfy all four requirements of Rule 23(a), and at least one of the sub-sections of Rule 23(b). *Comcast Corp. v. Behrend*,

569 U.S. 27, 33 (2013); *Zinser v. Accufix Research Inst., Inc.*, 253 F.3d 1180, 1186 (9th Cir. 2001), *amended by* 273 F.3d 1266 (9th Cir. 2001).

Rule 23(a) imposes four prerequisites. The class must be "so numerous that joinder of all members is impracticable" (numerosity). There must be "questions of law or fact common to the class" (commonality). The claims or defenses of the named plaintiffs must be "typical of the claims or defenses of the class" (typicality). And the named parties must show that they "will fairly and adequately protect the interests of the class" (adequacy). Fed. R. Civ. P. 23(a)(1)-(4).

To obtain a Rule 23(b)(3) class, plaintiffs must also must show that "questions of law or fact common to class members predominate over any questions affecting only individual members" (predominance) and that a class action is "superior to other available methods for fairly and efficiently adjudicating the controversy" (superiority). Fed. R. Civ. P. 23(b)(3).

The Court's "class-certification analysis must be rigorous and may entail some overlap with the merits of the plaintiff's underlying claim." *Amgen Inc. v. Connecticut Ret. Plans & Trust Funds*, 568 U.S. 455, 465-66 (2013) (internal quotations and citations omitted). "That is so because the class determination generally involves considerations that are enmeshed in the factual and legal issues comprising the plaintiff's cause of action." *Comcast,* 569 U.S. at 33-34 (internal quotations and citations omitted). These principles apply to the Rule 23(a) and 23(b) analysis alike. *Id.* at 34.

The rigorous analysis, however, has its limits. "Rule 23 grants courts no license to engage in free-ranging merits inquiries at the certification stage. Merits questions may be considered to the extent -- but only to the extent -- that they are relevant to determining whether the Rule 23 prerequisites for class certification are satisfied." *Amgen*, 586 U.S. at 466. The class certification procedure is decidedly not an alternative form of summary judgment or an occasion to hold a mini-trial on the merits. *Alcantar v. Hobart Service*, 800 F.3d 1047, 1053 (9th Cir. 2015). The goal under Rule 23 is "to select the metho[d] best suited to adjudication of the controversy fairly and efficiently." *Amgen*, 568 U.S. at 460 (internal quotations omitted) (modification in original). That means deciding whether efficiency and the interests of justice are best served by having the named plaintiffs go forward to the merits as individuals or on behalf of a class as "an exception to the usual rule that litigation is conducted by and on behalf of the individual named parties only." *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 348 (2011) (quoting *Califano v. Yamasaki*, 442 U.S. 682, 700-701 (1979)). *See generally Brickman v. Fitbit, Inc.*, No. 3:15-CV-02077-JD, 2017 WL 5569827, at *2-3 (N.D. Cal. Nov. 20, 2017).

The decision of whether to certify a class is entrusted to the sound discretion of the district court. *Zinser*, 253 F.3d at 1186.

DISCUSSION

I. The Initial Proposed Class

Plaintiffs initially propose a class consisting of all Illinois Facebook users appearing in a photograph uploaded to Facebook. This broad definition is not viable because it poses insurmountable problems with superiority and manageability, commonality, predominance, and is not "reasonably co-extensive with Plaintiffs' chosen theory of liability." *Torres v. Mercer Canyons Inc.*, 835 F.3d 1125, 1136-37 (9th Cir. 2016).

Simply appearing in an uploaded photograph does not necessarily mean that a face signature or template was collected or stored, or that any biometric data was harvested. As plaintiffs acknowledge, Facebook "locates certain landmarks on the face and uses that data to create a three-dimensional map of the face" only after the initial steps of detection and alignment are successfully completed. Dkt. No. 255 at 3. Unique physical characteristics are not involved in the detection step, which is about locating all faces rather than a specific face. The detection and alignment steps fail for approximately 24% of faces appearing in photographs. *See* Dkt. No. 284-9 ¶¶ 5-6. The uncertainty generated by this match failure rate is compounded by evidence in the record, which plaintiffs do not contest, that Facebook cannot reliably determine whether a face signature was ever computed from a particular photograph, *id.* ¶¶ 11-12, and that face signatures are not stored, Dkt. No. 256-8 ¶ 20. The record also shows that at times during the proposed class period, the software did not

consistently compute face signatures from a given photograph. *See* Dkt. No. 284-9 ¶ 12.

These uncontested facts establish that uploading a photo did not necessarily result in the collection of biometric data. Consequently, a class defined by uploaded photographs is too amorphous and potentially over-inclusive to be certified. *See Torres*, 835 F.3d at 1139; *Lozano v. AT & T Wireless Servs., Inc.*, 504 F.3d 718, 730 (9th Cir. 2007). Plaintiffs suggest that a vigorous claims process can fix these problems, but that only pushes them down the road to a later stage. Facebook will have no greater ability to resolve these uncertainties at the verification stage than at this definitional one. Plaintiffs' citations to claims procedure cases are inapposite for this reason. *See, e.g.*, *In re Cmty. Bank of N. Virginia Mortg. Lending Practices Litig.*, 795 F.3d 380, 397 (3d Cir. 2015) (defendant already possessed all relevant records and identification method was reliable and repeatable).

Plaintiffs also suggest that they can obtain certification on the theory that users with multiple photos posted on Facebook are likely to have had at least one processed in the representation or classification steps, where biometric data is collected. Dkt. No. 292 at 7. That too is inherently imprecise, and plaintiffs do not offer any statistical or other methods that might translate this presumed likelihood into a reasonably certain class definition.

II. The Certified Class

Plaintiffs' alternative proposal is tied to face templates, and with a minor modification it provides

a sound basis for certification. A class comprised of Facebook users located in Illinois for whom Facebook created and stored a face template after June 7, 2011, satisfies Rule 23's requirements and neutralizes most of Facebook's objections, which go mainly to problems caused by the use of face signatures to define the class. This definition modestly refines plaintiffs' alternative class proposal, and will be used for the remaining Rule 23 analysis. *See Armstrong v. Davis*, 275 F.3d 849, 871 n.28 (9th Cir. 2001) ("district court may redefine the class") (citing *Penk v. Oregon State Bd. of Higher Educ.,* 816 F.2d 458, 467 (9th Cir. 1987)), *abrogated on other grounds by Johnson v. California*, 543 U.S. 499 (2005).

A. Numerosity, Adequacy, and Typicality

The numerosity, adequacy, and typicality requirements in Rule 23(a) are readily satisfied for a template-based class of Illinois users. Plaintiffs reasonably estimate that millions of Illinois residents are Facebook users, many of whom have been tagged in enough photographs to have face templates. Dkt. No. 255 at 6. Plaintiffs' arguments are uncontested by Facebook, and numerosity is established.

Adequacy is also not an issue. Neither named plaintiffs nor their counsel have an apparent conflict of interest with other class members, and the hard-fought proceedings in this case amply establish that they will "prosecute the action vigorously on behalf of the class." *Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1020 (9th Cir. 1998). Facebook says adequacy cannot be found because the named plaintiffs "know almost nothing" about their case or claims, but that goes too

far. Dkt. No. 285 at 24. The deposition testimony by the named plaintiffs shows a perfectly adequate understanding of the case, and it clearly manifests their concerns about Facebook's treatment of personal biometric data. *See, e.g.*, Dkt. Nos. 255-5; 255-6; 284-23; 284-24; 284-25. This is not a situation where the named plaintiffs "are startlingly unfamiliar with the case." *Dufour v. Be LLC*, 291 F.R.D. 413, 419 (N.D. Cal. 2013) (internal quotations omitted). In any event, objections to adequacy based on a named representative's alleged ignorance are disfavored. *See Surowitz v. Hilton Hotels Corp.*, 383 U.S. 363, 370-74 (1966). Even if the named plaintiffs have relied heavily on the advice of attorneys and others, it is hardly a badge of inadequacy to seek help from those with relevant expertise, particularly in a complex case like this one. *Baffa v. Donaldson, Lufkin & Jenrette Sec. Corp.*, 222 F.3d 52, 62 (2d Cir. 2000).

There is no serious doubt that typicality is satisfied, too. Named plaintiffs are Illinois Facebook users with face templates suing under Illinois law on behalf of fellow users in Illinois. That is enough to "assure that the interest of the named representative aligns with the interests of the class." *Hanon v. Dataproducts Corp.*, 976 F.2d 497, 508 (9th Cir. 1992). Typicality may be a bar to certification if other members would suffer because the named plaintiffs would be "preoccupied with defenses unique to" them. *Just Film, Inc. v. Buono*, 847 F.3d 1108, 1116 (9th Cir. 2017) (quoting *Hanon*, 976 F.2d at 508). That is not the situation here. Facebook has not shown that named plaintiffs would be preoccupied

with unique defenses, or are in any way atypical with respect to the overall class.

B. Commonality and Predominance

The main thrust of Facebook's non-technical objections to certification go to the somewhat overlapping factors of commonality under Rule 23(a)(2) and predominance under Rule 23(b)(3). These inquiries go to the heart of whether adjudication of the claims on a class basis would be fair, efficient and superior to individual prosecution.

The commonality requirement is satisfied when "there are questions of law or fact common to the class." Fed. R. Civ. P. 23(a)(2). "Because any competently crafted class complaint literally raises common questions," the Court's task is to look for a common contention "capable of classwide resolution -- which means that determination of its truth or falsity will resolve an issue that is central to the validity of each one of the claims in one stroke." *Alcantar*, 800 F.3d at 1052 (internal quotations and citations omitted). What matters is the "capacity of a classwide proceeding to generate common *answers* apt to drive the resolution of the litigation." *Wal-Mart*, 564 U.S. at 350 (internal quotations omitted) (emphasis in original).

Rule 23(a)(2) does not demand total uniformity across a class. "All questions of fact and law need not be common to satisfy the rule. The existence of shared legal issues with divergent factual predicates is sufficient, as is a common core of salient facts coupled with disparate legal remedies within the class." *Hanlon*, 150 F.3d at 1019. Rule 23(a)(2)

imposes a "'rigorous' commonality standard." *Levya v. Medline Indus. Inc.*, 716 F.3d 510, 512 (9th Cir. 2013).

Rule 23(b)(3) requires that common questions of law or fact predominate over individual ones. The predominance inquiry asks whether "common questions present a significant aspect of the case and [if] they can be resolved for all members of the class in a single adjudication." *Hanlon*, 150 F.3d at 1022 (internal quotations omitted); *see also Tyson Foods v. Bouaphakeo*, __ U.S. __, 136 S.Ct. 1036, 1045 (2016). Each element of a claim need not be susceptible to classwide proof, *Amgen*, 568 U.S. at 468-69, and the "important questions apt to drive the resolution of the litigation are given more weight in the predominance analysis over individualized questions which are of considerably less significance to the claims of the class." *Torres*, 835 F.3d at 1134. Rule 23(b)(3) permits certification when "one or more of the central issues in the action are common to the class and can be said to predominate, . . . even though other important matters will have to be tried separately, such as damages or some affirmative defenses peculiar to some individual class members." *Tyson*, 136 S. Ct. at 1045 (internal quotations omitted).

As the Court has discussed in other decisions, the line separating the commonality inquiry under Rule 23(a)(2) and the predominance assessment under Rule 23(b)(3) can be elusive. *See Ochoa v. McDonald's Corp.*, Case No. 14-cv-02098 JD, 2016 WL 3648550, at *5-6 (N.D. Cal. July 7, 2016). *Wal-Mart* emphasized the commonality inquiry, but the Supreme Court has also advised that "[i]f anything,

Rule 23(b)(3)'s predominance criterion is even more demanding than Rule 23(a)." *Comcast*, 569 U.S. at 34. Whatever the precise demarcation might be between the two inquiries, it is clear that commonality alone will not fulfill Rule 23(b)(3), and that the main concern under subsection (b)(3) "is the balance between individual and common issues." *In re Hyundai and Kia Fuel Economy Litigation*, 881 F.3d 679, 691 (9th Cir. 2018) (internal quotations omitted); *see also Tyson*, 136 S.Ct. at 1045 (purpose of the Rule 23(b)(3) inquiry is to determine whether the proposed class is "sufficiently cohesive to warrant adjudication by representation") (quoting *Amchem Products, Inc. v. Windsor*, 521 U.S. 591, 623 (1997)). As a practical matter, commonality and predominance can be assessed in tandem, with a careful eye toward ensuring that the specific requirements of each are fully satisfied. *See, e.g.*, *Just Film*, 847 F.3d at 1120-21.

As an initial matter, there is no doubt that a template-based class poses common legal and factual questions, namely: did Facebook's facial recognition technology harvest biometric identifiers as contemplated under BIPA, and if so, did Facebook give users prior notice of these practices and obtain their consent? Facebook agrees that these questions reach the entire class, Dkt. No. 285 at 9, but challenges whether common answers will predominate. Specifically, Facebook contends that three issues can be resolved only by individualized evidence of: (1) whether a class member is "aggrieved" as that word is used in BIPA, which grants a private right of action only to "persons aggrieved" under it; (2) whether a class member's

claims fall within BIPA's territorial scope; and (3) whether a class member was depicted in photographs derived from "paper photos . . . converted to digital form before upload." *Id.*

Facebook puts greatest emphasis on its argument about the meaning of "aggrieved." It relies almost exclusively on *Rosenbach v. Six Flags Entertainment Corporation*, 2017 IL App (2d) 170317 (Ill. App. Ct. 2017), a currently unpublished opinion by an intermediate court of appeals in Illinois. The BIPA claim in *Rosenbach* arose out of the practice by the defendant amusement parks of fingerprinting season pass holders so that thumb scans could speed up entry into the park. The parks collected a minor's thumbprint when he purchased a pass, and his mother subsequently objected under BIPA that the parks had not provided prior notice or obtained consent. She sued on those grounds. The trial court initially denied defendants' motion to dismiss but certified questions about the meaning of "aggrieved" to the appellate court. *Rosenbach* is the intermediate court's response to the certified questions.

As a threshold matter, *Rosenbach* does not bear the heavy weight Facebook seeks to place on it. Facebook heatedly insists that *Rosenbach* interpreted "aggrieved" to require injury or harm "*beyond* the alleged statutory violation." Dkt. No. 285 at 1 (emphasis in original). But the opinion is far less pertinent or definitive than Facebook contends, and a fair reading suggests that the *Rosenbach* court would have reached the opposite conclusion had the allegations in this case been before it. *Rosenbach* states on several occasions that the plaintiff in that case -- the mother of the minor fingerprinted by the

amusement park defendants -- did not allege that she or her son "suffered any actual injury." *See, e.g.*, *Rosenbach*, 2017 IL App (2d) 170317, ¶ 10 ("Plaintiff alleged not that she or Alexander suffered any actual injury, but that, had she known of defendants' conduct, 'she never would have purchased a season pass for her son."). Instead, "the only injury alleged" by the plaintiff was "a violation of the notice and consent requirements of section 15(b) of the Act," and her argument was that "a mere technical violation of the Act is sufficient to render a party 'aggrieved.'" *Id.* ¶ 18. Critically, the *Rosenbach* court expressly observed that "Plaintiff did not allege in her complaint any harm or injury to a privacy right," *id.* ¶ 20 n.1, and underscored that the "injury or adverse effect need not be pecuniary" to qualify a person as "aggrieved" under BIPA. *Id.* ¶ 28. Facebook glosses over these essential parts of *Rosenbach* to say it demands some undefined "actual" harm beyond injury to a privacy right, but the better reading is *Rosenbach* would find that injury to a privacy right is enough to make a person aggrieved under BIPA. As the Court has already found, there is no question that plaintiffs here have sufficiently alleged that intangible injury. *See, e.g.*, Dkt. No. 40 ¶ 17 (Facebook "continues to violate millions of Illinois residents' legal privacy rights"); *id.* ¶ 31.

This is enough to overcome Facebook's objections based on its interpretation of *Rosenbach.* To the extent *Rosenbach* might be read differently, the Court would part company with it. To be sure, principles of comity and federalism counsel that federal courts should not lightly disregard state court interpretations of state law. But as an intermediate

court opinion, *Rosenbach* is a non-binding data point for ascertaining Illinois law, and if "other persuasive data" convinces the Court that the Illinois Supreme Court would decide otherwise, the Court need not follow it. *Am. Tower Corp. v. City of San Diego*, 763 F.3d 1035, 1047 (9th Cir. 2014); *Klein v. United States*, 537 F.3d 1027, 1032 (9th Cir. 2008).

A considerable amount of "persuasive data" would indeed call into serious doubt an intermediate court decision holding that BIPA requires "actual" injury beyond an invasion of privacy. First and foremost is the plain language of BIPA itself. As the Illinois Supreme Court has held, the "cardinal rule in interpreting a statute is to give effect to the intent of the legislature." *People v. Fort*, 88 N.E.3d 718, 723 (Ill. 2017) (internal citation omitted). The legislature's intent is best determined from the language of the statute itself, which should be read as a whole to determine "its nature, its object and the consequences that would result from construing it one way or the other." *Id.* at 723-724 (internal quotations omitted); *see also FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 132-33 (2000) ("fundamental canon of statutory construction" to define words in reference to "context" and "overall statutory scheme") (quoting *Davis v. Michigan Dept. of Treasury*, 489 U.S. 803, 809 (1989)).

These well-established canons of interpretation are crucial here, because a plain of reading of BIPA "leave[s] little question that the Illinois legislature codified a right of privacy in personal biometric information" rooted in "a long tradition of claims actionable in privacy law" and extending to control

over one's data, independent of disclosure or misuse risks. *Patel,* 2018 WL 1050154, at *4. This intent cannot be squared with a construction of "aggrieved" that requires some other "actual" injury, whatever that might be, particularly when deprivation of BIPA's notice and consent requirements amounts to the "precise harm the Illinois legislature sought to prevent." *Id.* Such a holding would be all the more questionable because the Illinois legislature clearly knows how to condition a cause of action on actual injury simply by saying so in the statute. *See, e.g.*, 815 Ill. Comp. Stat. Ann. 505/10a (Illinois Consumer Fraud and Deceptive Business Practices Act) (private right of action limited to person who suffers "actual" damage). The legislature did not choose to say so in BIPA, and that choice must be given weight.

This statutory analysis would be enough on its own to turn away Facebook's characterization of *Rosenbach*. *See Am. Tower*, 763 F.3d at 1047 (text of statute alone is persuasive data). Express precedent from the Illinois Supreme Court is another point of persuasive data against it. The Illinois high court has determined that "aggrieved" parties under an Illinois statute are those with a "direct, immediate and substantial interest rather than a speculative, theoretical, inconsequential or remote interest." *Am. Sur. Co. v. Jones*, 384 Ill. 222, 230 (Ill. 1943). The Illinois Supreme Court made this determination in the context of an insurance statute, but did not cabin its holding to that statute or the facts before it. *Jones* stands for the proposition that, under Illinois law, an individual is "aggrieved" when "a legal right is invaded by the act complained of." *Id.* at 229-230 (quoting *Glos v. People*, 259 Ill. 332, 340 (Ill. 1913)).

Tellingly, *Rosenbach* omits any discussion of *Jones,* and Facebook also does not address it in its papers. That is a concern because *Jones* is good law in Illinois and is actively cited today by other federal courts and Illinois state courts, significantly in the BIPA context. *See, e.g.*, *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499, 520 (S.D.N.Y. 2017) (citing *Jones* in interpreting BIPA). A convincing construction of "aggrieved" in BIPA would need to account for *Jones,* and not rely entirely, for example, on decisions from courts outside Illinois. *See, e.g., Rosenbach*, 2017 IL App (2d) 170317, ¶ 22 (citing Wisconsin decision).

An analysis of *Jones is* particularly important because a good argument can be made that Facebook's reading of *Rosenbach is* not consistent with it. *Jones* holds that a party is aggrieved by an act that directly or immediately affects her legal interest. In contrast, Facebook portrays *Rosenbach* as saying that the word "aggrieved" requires a plaintiff to affirmatively plead some additional "actual injury" as an element of her claim, whatever that undefined extra harm might be. Dkt. No. 285 at 10. This is a significantly more limited construction of "aggrieved" than afforded by *Jones,* and the grounds on which it can be harmonized with *Jones* are not at all clear.

It is also worth noting that the facts in *Rosenbach* place it several steps away from this case. In *Rosenbach,* the plaintiff's son provided his thumbprint for scanning by the defendant. *Rosenbach*, 2017 IL App (2d) 170317, ¶ 7. As the *Spokeo* order discussed, an express request for a fingerprint scan is a far cry from the situation here,

where plaintiffs plausibly argue that simply using Facebook or reading Facebook's user policy did not put them on notice that Facebook was collecting their biometric data. *See Patel*, 2018 WL 1050154, at *5 (distinguishing fingerprinting cases). Indeed, an Illinois trial court has applied *Rosenbach* to dismiss a BIPA case precisely because the plaintiff expressly allowed defendants to take a fingerprint scan and so could not plead an invasion of privacy. *Rottner v. Palm Beach Tan, Inc., et al.*, No. 15 CH 16695 (Ill. Cir. Ct. Mar. 2, 2018) (available at Dkt. No. 315-1).

Consequently, if *Rosenbach* were to be read as Facebook urges, persuasive data convinces the Court it would not be a good prediction of how the Illinois Supreme Court would interpret "aggrieved" under BIPA. It follows that Facebook has not demonstrated on the basis of *Rosenbach* that a predominance of individual inquiries would defeat class certification.

Facebook's other commonality and predominance objections also pose no certification bar. Facebook raises an "extraterritoriality" contention based on the assertion that its servers are not located within Illinois. The parties agree that BIPA does not have extraterritorial reach because no "clear intent in this respect appears from the express provisions of the statute," *Avery v. State Farm Mut. Auto. Ins. Co.*, 216 Il1.2d 100, 185 (Ill. 2005), but disagree how that applies here.[1]

---

[1] Facebook raises a similar argument in its motion for summary judgment. The Court considers it here with respect to certification only.

There is no genuine dispute that this case is deeply rooted in Illinois. The named plaintiffs are located in Illinois along with all of the proposed class members, and the claims are based on the application of Illinois law to use of Facebook mainly in Illinois. As the Court found in a prior order, the case is properly governed by Illinois law pursuant to California choice of law principles, *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1169 (N.D. Cal. 2016), and Facebook does not contest the application of Illinois law in opposing class certification. None of the class members are non-residents suing under Illinois law, which is the paradigmatic situation for the presumption against the extraterritorial application of local law. *See, e.g.*, *Avery*, 216 Ill.2d at 187. Facebook has not tendered any evidence to indicate that the circumstances relating to the challenged conduct did not occur "primarily and substantially within" Illinois. *Id.* Class members do not need to show more in order to sue under BIPA, particularly in light of BIPA's express concerns about data collection by "[m]ajor national corporations," 740 Ill. Comp. Stat. Ann. 14/5(b). *See Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 267 (2010) (territoriality inquiry looks to the "objects of the statute's solicitude").

Contrary to Facebook's suggestion, the geographic location of its data servers is not a dispositive factor. Server location may be one factor in the territoriality inquiry, but it is not the exclusive one. As *Avery* cautions, "focusing solely on [only one circumstance] . . . can create questionable results" where "the bulk of the circumstances . . . occur within Illinois." *Avery*, 216 Ill.2d at 186; *see also Rivera v. Google Inc.*, 238

F. Supp. 3d 1088, 1102 (N.D. Ill. 2017) (in BIPA face scan context, even if "the scanning takes place outside of Illinois, that would not necessarily be dispositive"). *Avery's* warning is particularly apt here because the functionality and reach of modern online services like Facebook's cannot be compartmentalized into neat geographic boxes. Making the geographic coordinates of a server the most important circumstance in fixing the location of an Internet company's conduct would yield the questionable results *Avery* counsels against. Among other problematic outcomes, it would effectively gut the ability of states without server sites to apply their consumer protection laws to residents for online activity that occurred substantially within their borders. *See Rocky Mountain Farmers Union v. Corey*, 730 F.3d 1070, 1104 (9th Cir. 2013) (state cannot "impose its own regulatory standards on another jurisdiction" but "may regulate with reference to local harms"). Correlatively, a single-minded focus on server location would also potentially nationalize the consumer protection laws of states that host servers, which in this case includes California. Both outcomes are fraught with unintended and undesirable consequences.

Facebook also suggests that the claims of some class members may only be peripherally related to Illinois. It says for example that some class members might have just moved to Illinois with face templates created elsewhere. Dkt. No. 285 at 18. Maybe so, but Facebook does not offer anything other than its own conjecture on this point, and mere "speculation" about class variability "does not meet [defendant's] burden of demonstrating that individual . . . issues

predominate." *Gutierrez v. Wells Fargo Bank, NA*, 704 F.3d 712, 729 (9th Cir. 2012).

As a final contention, Facebook says that predominance cannot be found because individualized inquiries may be necessary to determine which users' face templates were derived from scans of paper photographs. This too is unavailing. Assuming for discussion purposes only that a class member's claim could turn on whether an uploaded photograph was taken by a digital versus film camera, Facebook simply asserts with no accompanying evidence that "[m]any photos uploaded to Facebook fit that description." Dkt. No. 285 at 19. Conclusory allegations with no support in the record will not defeat commonality and predominance. *Brickman*, 2017 WL 5569827, at *5.

C. Superiority

The closing consideration for certification is whether any fairness or practical case management reasons count against it. "Rule 23(b)(3) requires that a class action be 'superior to other available methods for fairly and efficiently adjudicating the controversy,' and it specifically mandates that courts consider 'the likely difficulties in managing a class action.'" *Briseno v. ConAgra Foods, Inc.*, 844 F.3d 1121, 1127-28 (9th Cir. 2017).

A class action is clearly superior to individual proceedings here. While not trivial, BIPA's statutory damages are not enough to incentivize individual plaintiffs given the high costs of pursuing discovery on Facebook's software and code base and Facebook's willingness to litigate the case. *Just Film*, 847 F.3d

at 1123. The class will be manageable because members can be identified in a straightforward way. Facebook has collected a wealth of data on its users, including self-reported residency and IP addresses. *See* Dkt. No. 255 at 7. Facebook does not argue that determining the location of Facebook users with face templates would be unduly difficult or subject to significant uncertainty.

Facebook seems to believe that a class action is not superior because statutory damages could amount to billions of dollars. Dkt. No. 285 at 20. To be sure, class certification may be inappropriate where it would result in damages inconsistent with legislative intent. *Bateman v. Am. Multi-Cinema, Inc.*, 623 F.3d 708, 722-23 (9th Cir. 2010); *Kline v. Coldwell, Banker & Co.*, 508 F.2d 226, 235 (9th Cir. 1974). But the Illinois legislature knows how to speak clearly when it wants to foreclose class actions. *See, e.g.*, 35 Ill. Comp. Stat. 200/23-15(a) ("no complaint shall be filed as a class action"). Facebook suggests that BIPA's limitation of relief to "aggrieved" persons bespeaks a reluctance to impose hefty penalties on non-compliant companies, but it offers no evidence or cogent explanation in support of that claim, and to the extent it relies on *Rosenbach,* the argument is rejected for the previously stated reasons. In addition, substantial damages are not a reason to decline class certification because it is within the Court's discretion to reduce a liquidated damages award to comport with due process at a later stage of the proceedings. *See, e.g.*, *Six (6) Mexican Workers v. Arizona Citrus Growers*, 904 F.2d 1301, 1309 (9th Cir. 1990).

CONCLUSION

The Court certifies a class of Facebook users located in Illinois for whom Facebook created and stored a face template after June 7, 2011.

IT IS SO ORDERED.

Dated: April 16 2018

/s/ James Donato
JAMES DONATO
United States District Judge

APPENDIX D

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

No. 18-15982

NIMESH PATEL, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED; ET AL.,
Plaintiff-Appellees,

v.

FACEBOOK, INC.,
Defendant-Appellant.

Filed: October 18, 2019

D.C. No. 3:15-cv-03747-JD
Northern District of California, San Francisco

ORDER

Before: GOULD and IKUTA, Circuit Judges, and PEARSON,* District Judge.

Judge Gould and Judge Ikuta voted to deny the petition for rehearing en banc and Judge Pearson so

---

* The Honorable Benita Y. Pearson, United States District Judge for the Northern District of Ohio, sitting by designation.

recommended. The petition for rehearing en banc was circulated to the judges of the court, and no judge requested a vote for en banc consideration.

The petition for rehearing en banc is DENIED.

APPENDIX E

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE FACEBOOK BIOMETRIC INFORMATION PRIVACY LITIGATION

THIS DOCUMENT RELATES TO: ALL ACTIONS

FREDERICK WILLIAM GULLEN, ON BEHALF OF HIMSELF AND ALL OTHERS SIMILARLY SITUATED,

Plaintiff,

v.

FACEBOOK, INC.,

Defendant.

DECLARATION OF OMRY YADAN IN SUPPORT OF FACEBOOK, INC.'S MOTION FOR SUMMARY JUDGMENT

Master Docket No.: 3:15-CV-03747-JD

Hon. James Donato

Case No. 3:16-cv-00937-JD

Filed: 12/08/2017

---

* * *

Facebook's Data Centers

6. The computers, servers, and databases used to provide services to people with Facebook accounts are located in nine "Data Centers" maintained by Facebook. Six Data Centers are located within the United States, in (i) Prineville, Oregon ("PRN"), (ii) Santa Clara, California ("SNC"), (iii) Altoona, Iowa ("ATN"), (iv) Fort Worth, Texas ("FTW"), (v) Ashburn, Virginia ("ASH"), and (vi) Forest City, North Carolina ("FRC"). Attached as Exhibit 1 (FBBIPA_00044570) is a true and correct copy of excerpts from an internal "Wiki" page maintained by Facebook that shows the location of each current Data Center, and additional data centers that are now under construction.

7. None of Facebook's Data Centers is located in Illinois, nor has Facebook maintained any Data Centers in Illinois at any point since Facebook first began using facial-recognition technology in 2010. Facebook is in the process of developing additional Data Centers in the United States and in other countries, but none is in Illinois.

8. In addition, none of the Facebook or former Face.com employees involved in developing Facebook's facial-recognition technology, or the facial-recognition technology that Facebook initially licensed from Face.com, is based in Illinois, nor are any of the Facebook employees who work with that technology today based in Illinois. None of the work that has ever been done to design, engineer, or

implement Facebook's facial-recognition technology has taken place in Illinois.

* * *

APPENDIX F

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE FACEBOOK BIOMETRIC INFORMATION PRIVACY LITIGATION

THIS DOCUMENT RELATES TO: ALL ACTIONS

Case No. 3:15-cv-03747-JD

Hon. James Donato

CONFIDENTIAL

VOLUME II

VIDEOTAPED DEPOSITION OF NIMESH PATEL

Chicago, Illinois

Thursday, December 7, 2017

[pp. 132:18-135:16]

* * *

Q. Has your use of Facebook changed at all since you filed this lawsuit?

A. No.

Q. Do you avoid any features?

A. No.

Q. Have your photo uploading practices changed at all since you filed this suit?

A. No.

Q. When you upload photographs, do you tag people?

A. Yes.

Q. Do you tag more or less often since filing the suit, or about the same?

A. Probably – I'm not sure. Don't remember how I did before.

Q. But you – currently you tag people with some frequency?

A. Yes.

MR. WILLIAMS: Objection. Form.

Q. And so, I just want to drill down on that a little bit. So you receive tag suggestions when you upload certain photographs; right?

A. Yes.

Q. And do you – have you tagged friends based on tag suggestions you receive?

A. Yes.

Q. Is that a helpful feature that Facebook offers?

MR. WILLIAMS: Objection. Form.

A. It's a nice feature.

Q. And you – it's nice because it saves you the trouble of having to manually tag one of your friends; correct?

A. Yeah, yes.

Q. But tag suggestions isn't telling you any information you don't already know, is it?

A. No.

Q. Meaning you know – it's showing you your friends in the photographs; right?

A. Right.

Q. And you know what your friends look like?

A. Yes.

Q. Do you receive notifications from Facebook if another user tags you in a photograph?

A. I don't know.

Q. You've never received any type of notification that's –

A. I might have, but I don't remember.

Q. Do you find that to be a helpful feature, knowing that other friends have tagged you?

A. Yes.

Q. Have you ever contacted one of your friends and asked them to remove a tag or a picture of you from Facebook?

A. No.

Q. When you – do you ever review the tags of yourself?

A. No.

Q. Are you aware that you can untag yourself from posts?

A. I'm aware of it, but I'm not a hundred percent sure.

Q. But you've never done it?

A. No, I have never done it, at least that's what I remember.

Q. You realize you can opt out of tag suggestions; correct?

A. I believe so.

Q. But you've never done that, have you?

A. No, I have not done that.

Q. How come?

A. Not sure.

Q. Is it because you like the feature?

A. The feature's nice.

* * *

APPENDIX G

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE FACEBOOK BIOMETRIC INFORMATION
PRIVACY LITIGATION

THIS DOCUMENT RELATES TO: ALL ACTIONS

Case No. 3:15-cv-03747-JD

CONFIDENTIAL

VOLUME II

VIDEOTAPED DEPOSITION OF CARLO LICATA

Chicago, Illinois

Tuesday, October 24, 2017

[p. 146:13-24]

* * *

Q. Do you believe that you've been harmed at all by tag suggestions?

A. I'm unaware if I ever have or not.

Q. Okay. So that means -- are you aware of losing any money because of facial recognition or tag suggestions on Facebook?

A. No, I'm not.

Q. Losing any property?

A. No.

Q. Are you aware of any other harm because of facial recognition or tag suggestions on Facebook?

A. Not to my knowledge.

* * *

APPENDIX H

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE FACEBOOK BIOMETRIC INFORMATION PRIVACY LITIGATION

THIS DOCUMENT RELATES TO: ALL ACTIONS

Case No. 3:15-cv-03747-JD

CONFIDENTIAL

VOLUME II

VIDEOTAPED DEPOSITION OF ADAM PEZEN

Chicago, Illinois

Tuesday, October 24, 2017

[pp. 172:7-174:21]

* * *

Q. Okay. Do you feel you're being harmed in some way by tag suggestion?

A. Harmed? Um --

MR. RHODES: Objection to the extent it calls for a legal conclusion.

Go ahead.

A. Being that I don't know details behind it, I -- yeah, I could only speculate as to the actual risk. That's sort of my concern.

Q. But as you sit there, can you identify any actual harm you've suffered because of tag suggestion?

MR. RHODES: Objection. Vague. Calls for a legal conclusion.

A. I'm neither a doctor nor a psychiatrist either. I couldn't say.

Q. Are you able to articulate any injuries you're seeking to recover for?

MR. RHODES: Same objections.

A. I'm articulate.

Q. No.

A. Again --

Q. I'm asking you, like, can you list for me the injuries you're looking to recover for?

A. It would --

MR. RHODES: Objection.

A. Yeah, it would all be -- it's -- it's information that I'm looking for. It's not knowing what is going on more than injuries.

Q. Okay. So you can't identify any particular injury, it's just you want more information from Facebook?

MR. RHODES: Objection. Mischaracterizes testimony.

Q. Is that what you're saying?

A. Um, if I or someone else were being harmed, the fact that -- through this process of facial data collection, it's all the more reason that that be made explicit, the collection.

Q. But I want to move out of the realm of speculation. You started your answer with "if someone was being harmed." I want to know if you actually have been harmed. Are you able to identify for me any type of harm you've actually suffered?

MR. RHODES: Objection. Compound. Vague. Calls for a legal conclusion.

Q. Have you lost money because of tag suggestions?

A. I don't know.

Q. Have you lost property because of tag suggestions?

A. I don't know. I mean, and these things seem totally plausible in certain circumstances, but it would all be speculation.

Q. Okay. So, and I don't want you to speculate.

A. Yes.

Q. Can you identify any money or property you have lost because of tag suggestions?

A. No.

Q. Okay. Can you identify any other harm that has occurred to you because of tag suggestions?

MR. RHODES: Objection. Vague. Calls for a legal conclusion.

A. I personally, no.

* * *