FOR PUBLICATION

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

---

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

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 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.

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

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), Rafey S. Balabanian, and Lily Hough, Edelson PC, San Francisco, California; Jay Edelson, Benjamin Richman, and Alexander G. Tievsky, Edelson PC, Chicago, Illinois; Susan K. Alexander, Shawn A. Williams, and John George, Robbins Geller Rudman & Dowd LLP, San Francisco, California; Patrick J. Coughlin, Ellen Gusikoff Stewart, Lucas F. Olts, and Randi D. Bandman, Robbins Geller Rudman & Dowd LLP, San Diego, California; Paul J. Geller, Stuart A. Davidson, and Christopher C. Gold, Robbins Geller Rudman & Dowd LLP, Boca Raton, Florida; Lawrence Sucharow, Michael P. Canty, Corban S. Rhodes, and Ross Kamhi, 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 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.

---

[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/.

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.

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,

[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.

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 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

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

---

> 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).

[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.*

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

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

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 Torts

[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
>
> (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.

§ 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).

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 "long-standing 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 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.

[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.

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.