

No. 18-15982

---

---

IN THE

**United States Court of Appeals for the Ninth Circuit**

IN RE FACEBOOK BIOMETRIC PRIVACY LITIGATION

NIMESH PATEL, *et al.*,

*Plaintiffs-Appellees,*

v.

FACEBOOK, INC.,

*Defendant-Appellant.*

---

On Appeal from the United States District Court  
for the Northern District of California  
No. 3:15-cv-03747-JC

---

---

**BRIEF FOR *AMICUS CURIAE* INTERNET ASSOCIATION  
IN SUPPORT OF DEFENDANT-APPELLANT FACEBOOK, INC.'S  
PETITION FOR REHEARING EN BANC**

---

---

Susan D. Fahringer  
Nicola C. Menaldo  
Ryan Spear  
PERKINS COIE LLP  
1201 Third Avenue, Suite 4900  
Seattle, WA 98101  
Telephone: (206) 359-8000

Sunita Bali  
PERKINS COIE LLP  
505 Howard Street, Suite 1000  
San Francisco, CA 94105  
Telephone: (415) 344-7000

*Attorneys for Amicus Curiae*

## **CORPORATE DISCLOSURE STATEMENT**

Internet Association is a trade association representing leading global internet companies on matters of public policy. Internet Association does not have any parent corporations and does not issue stock.

## TABLE OF CONTENTS

	Page
CORPORATE DISCLOSURE STATEMENT .....	i
TABLE OF CONTENTS .....	ii
TABLE OF AUTHORITIES .....	iii
STATEMENT OF COMPLIANCE WITH RULE 29 .....	1
IDENTITY AND INTEREST OF <i>AMICUS CURIAE</i> .....	1
INTRODUCTION AND SUMMARY OF THE ARGUMENT .....	2
ARGUMENT.....	3
I. THE PANEL’S AFFIRMANCE OF THE DISTRICT COURT’S CLASS CERTIFICATION ORDER IGNORES THE TERRITORIAL LIMITS OF BIPA AND THREATENS TO IMPOSE A SINGLE STATE’S LAW NATIONWIDE. ....	3
A. The Panel Affirmed the Class Certification Order Even Though the Question of Whether BIPA Applies Necessarily Requires Consideration of Unique Facts Specific to Each Class Member.....	4
B. The Panel’s Opinion Extends BIPA Nationwide.....	10
II. VITIATING ARTICLE III STANDING REQUIREMENTS WOULD HAVE A SUBSTANTIAL AND DELETERIOUS IMPACT ON THE ASSOCIATION’S MEMBERS. ....	14
CONCLUSION .....	18

**TABLE OF AUTHORITIES**

**Page(s)**

**CASES**

*Avery v. State Farm Mut. Auto. Ins. Co.*,  
835 N.E.2d 801 (Ill. 2005).....5, 9, 10, 12

*BMW of N. Am., Inc. v. Gore*,  
517 U.S. 559 (1996).....12

*Califano v. Yamasaki*,  
442 U.S. 682 (1979).....9

*Comcast Corp. v. Behrend*,  
569 U.S. 27 (2013).....7

*Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades  
Council*,  
485 U.S. 568 (1988).....13

*Graham v. Gen. U.S. Grant Post No. 2665, V. F. W.*,  
248 N.E.2d 657 (1969) .....11

*Healy v. Beer Inst.*,  
491 U.S. 324 (1989).....13

*Mazza v. Am. Honda Motor Co., Inc.*,  
666 F.3d 581 (9th Cir. 2012) .....14

*Monroy v. Shutterfly, Inc.*,  
No. 16-C-10984, 2017 WL 4099846  
(N.D. Ill. Sept. 15, 2017) .....11

*Rivera v. Google Inc.*,  
238 F. Supp. 3d 1088 (N.D. Ill. 2017).....11

*Sam Francis Found. v. Christies, Inc.*,  
784 F.3d 1320 (9th Cir. 2015) (en banc) .....13

<i>Shady Grove Orthopedic Assoc. v. Allstate Ins. Co.</i> , 559 U.S. 393 (2010).....	8
<i>State Farm Mut. Auto Ins. Co. v. Campbell</i> , 538 U.S. 408 (2003).....	15
<i>Wal-Mart Stores, Inc. v. Dukes</i> , 564 U.S. 338 (2011).....	7
<i>Wilson v. Dep’t of Revenue</i> , 169 Ill. 2d 306 (1996) .....	13
<b>STATUTES</b>	
Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1, <i>et seq.</i> .....	passim
Cal. Civ. Code § 1798.100, <i>et seq.</i> .....	15
Wash. Rev. Code 19.375.010(5).....	21
<b>RULES</b>	
Fed. R. App. P. 35 .....	4
Fed. R. Civ. P. 23 .....	passim
Fed. R. Civ. P. 59.....	8
Fed. R. Civ. P. 60.....	8
<b>OTHER AUTHORITIES</b>	
Don Reisinger, <i>How Technology May Make Guns Safer</i> , Fortune (Dec. 3, 2015) .....	20
Emily Ann Brown, <i>Benefits of Biometrics</i> (Mar. 19, 2019), District Administration, <a href="https://districtadministration.com/biometric-security-boosts-school-safety-efficiency/">https://districtadministration.com/biometric-security-boosts-school-safety-efficiency/</a> .....	20

PR Newswire, *IBM Future of Identity Study: Millennials Poised to Disrupt Authentication Landscape* (Jan. 29, 2018), <https://www.prnewswire.com/news-releases/ibm-future-of-identity-study-millennials-poised-to-disrupt-authentication-landscape-300589262.html> ..... 19

Stephan Rabimov, *Evolution on Lock: From Stick to Gate*, Forbes (Dec. 27, 2017, 5:42 PM) ..... 20

## **STATEMENT OF COMPLIANCE WITH RULE 29**

No party or party's counsel authored this brief in whole or in part, and no such party or party's counsel made a monetary contribution intended to fund the preparation or submission of this brief. No one other than *amicus curiae*, its members, or its counsel made a monetary contribution to fund this brief's preparation or submission. Although Defendant-Appellant Facebook, Inc. is a member of Internet Association, Facebook did not author any part of this brief or make any monetary contribution to fund its preparation or submission.<sup>1</sup>

## **IDENTITY AND INTEREST OF *AMICUS CURIAE***

Internet Association (the "Association") represents more than 40 of the world's leading technology companies, from social networking services and search engines to travel sites and online marketplaces. The Association advances policies that protect internet freedom, promote innovation, and empower small businesses and the public. The panel's opinion threatens these values while providing little resulting benefit to consumer privacy. The panel's opinion also renders technology companies across the country, including many of the Association's members, uniquely vulnerable to baseless and abusive litigation under Illinois' Biometric Information Privacy Act ("BIPA"), 740 Ill. Comp. Stat. 14/1, *et seq.*

---

<sup>1</sup> Perkins Coie LLP represents Facebook in unrelated matters and has received no money from Facebook to prepare or submit this brief. All parties have consented to the filing of this brief.

BIPA imposes certain obligations on the collection and possession of biometric data that are unique to Illinois, and that are enforceable through a private right of action. En banc review is urgently needed to protect internet freedom, encourage innovation, and guard against abuse of the litigation process.

### **INTRODUCTION AND SUMMARY OF THE ARGUMENT**

The panel’s opinion addresses a question of exceptional importance to the hundreds of companies who are currently facing class action litigation under Illinois’ Biometric Information Privacy Act (“BIPA”), 740 Ill. Comp. Stat. 14/1, *et seq.*, as well as the countless others who will soon be in this statute’s crosshairs. That question is: May a plaintiff asserting a claim under BIPA obtain certification of a class defined as individuals “located in” that state—without a determination that any violation occurred in the state and without showing that any class member suffered harm? In answering this question with a resounding “yes,” the panel abrogated its responsibility to enforce the requirements for class certification under Federal Rule of Civil Procedure (“Rule”) 23, did so in a way that effectively extends BIPA nationwide, and misinterpreted the Supreme Court’s Article III jurisprudence.

The result of the panel’s opinion will be to force costly settlements—even in cases that lack merit—because many companies cannot risk classwide liability, no matter how strong their defenses. This is especially true for privacy statutes

like BIPA that contain generous statutory damages and fee-shifting provisions. And if the mere fact that class members may be “located in” a state is enough to certify a class based on alleged violations of that state’s privacy laws, then online companies will have no choice but to engage in overcompliance with those laws. That, in turn, would effectively extend those laws well beyond the state’s borders, raising questions under the dormant Commerce Clause. The panel’s Article III ruling, which essentially guarantees Article III standing to any plaintiff who can frame his claim as a “violation of privacy,” exacerbates that problem and invites abusive litigation by allowing plaintiffs to unlock BIPA’s generous remedial provisions without any showing of harm whatsoever.

The panel’s opinion merits en banc review under Federal Rule of Appellate Procedure 35 to ensure conformity with Rule 23 and Article III, and to resolve exceptionally important questions regarding how courts in the Ninth Circuit should handle privacy class actions arising under BIPA and other state laws.

## **ARGUMENT**

### **I. THE PANEL’S AFFIRMANCE OF THE DISTRICT COURT’S CLASS CERTIFICATION ORDER IGNORES THE TERRITORIAL LIMITS OF BIPA AND THREATENS TO IMPOSE A SINGLE STATE’S LAW NATIONWIDE.**

In affirming the district court’s class certification order, the panel failed to apply Rule 23(b)(3)’s predominance requirement, abdicating its duty to ensure that

the class was properly certified and interpreting BIPA in a manner that raises questions under the U.S. Constitution. Op. 22. The rules governing certification of privacy class actions arising under state law are of exceptional importance to companies that offer online services nationwide. So too is the geographic reach of state laws, like BIPA. The panel's decision merits en banc review for these reasons alone.

**A. The Panel Affirmed the Class Certification Order Even Though the Question of Whether BIPA Applies Necessarily Requires Consideration of Unique Facts Specific to Each Class Member.**

On appeal, Facebook argued that common questions did not predominate under Rule 23(b)(3) because (1) BIPA does not apply extraterritorially, and therefore putative class members could invoke BIPA only if they suffered a violation in Illinois; (2) under Illinois law, a violation occurs in the state only if the relevant series of events occurred “primarily and substantially” in Illinois, *see Avery v. State Farm Mut. Auto. Ins. Co.*, 835 N.E.2d 801, 854 (Ill. 2005); (3) determining whether a series of events occurs “primarily and substantially” in Illinois requires a fact-laden, multifactor analysis; and thus (4) determining whether each putative class member suffered a BIPA violation in Illinois necessarily turned on individualized questions that defeated Rule 23's predominance requirement. ECF No. 31-1 at 33.

Ignoring the fact-specific analysis required under Illinois law, the panel held that the location where “the violation of BIPA occurred” is a question of statutory interpretation that can be decided on a classwide basis. Op. 22. The panel then affirmed class certification without *deciding* that question. *Id.* at 23 n.7. It further observed that, “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.” *Id.* at 23.

The panel’s analysis is fraught with error and will have severe consequences for online service providers and others. The panel abrogated its duty to properly enforce Rule 23 at the class certification stage. It thereby departed from the precedent of this Court and the U.S. Supreme Court, meriting en banc review.

The panel observed, correctly, that “[t]he parties’ dispute regarding extraterritoriality requires a decision as to where the essential elements of a BIPA violation takes place.” Op. 22. And it recognized that at least some answers to that question could mean that common issues do not predominate. *Id.* at 23 (“future decisions . . . [could] lead to the conclusion that extraterritoriality must be evaluated on an individual basis”). The panel nonetheless *affirmed* class certification, holding that the *legal* question—not the *application* of the law to the facts—could be answered on a classwide basis. *Id.*

The panel’s decision turns Rule 23 on its head. A court may not simply presume that class treatment is appropriate and defer a rigorous predominance analysis until after certifying the class. Rather, *before* a class is certified, a court must determine 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); *Comcast Corp. v. Behrend*, 569 U.S. 27, 33 (2013) (“[A] party seeking to maintain a class action must affirmatively demonstrate his compliance with Rule 23.”) (citing *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 351 (2011)). Here, however, the panel did not analyze whether common issues predominated because it recognized that such an analysis would require determining whether the putative class members’ alleged BIPA violations occurred “primarily and substantially” in Illinois, and the district court had not made that determination. The panel dodged the issue and held that it was enough to state the legal test that should be applied—without applying it to the facts of the case. This not only flouts the requirement that a court must determine whether common issues predominate *before* certifying a class, it gives short shrift to the “rigorous analysis” the U.S. Supreme Court demands in cases seeking class treatment. *Dukes*, 564 U.S. at 350.

The panel dismissed any predominance concerns on the theory that if it *later* became clear that common issues did not predominate, then the class could be decertified. But the fact that decertification remains available at an (unidentified)

later stage in the proceedings does not cure the panel’s failure to enforce basic Rule 23 requirements. Courts can reconsider a wide range of decisions if the circumstances demand it. *See, e.g.*, Fed. R. Civ. P. 59, 60. The purpose of these safety valves, however, is to allow courts to remedy errors, not to kick down the road threshold issues—like the viability of a class—that can have massive consequences for how the dispute is litigated and ultimately resolved. *See Shady Grove Orthopedic Assoc. v. Allstate Ins. Co.*, 559 U.S. 393, 445 n.3 (2010) (“A court’s decision to certify a class . . . places pressure on the defendant to settle even unmeritorious claims.”) (Ginsburg, J., dissenting with Breyer, Kennedy, and Alito, JJ.). In addition, relying on the decertification procedure shifts the burden of proof regarding the appropriateness of class certification from the plaintiff to the defendant, which runs counter to the basic premise that a class action is “an exception to the usual rule that litigation is conducted by and on behalf of the individual named parties only.” *Califano v. Yamasaki*, 442 U.S. 682, 700-01 (1979).

Relatedly, the panel erred when it concluded that the district court would “not need to have mini-trials” once it determined “on a classwide basis” where the BIPA violation occurred. Op. 22-23. The panel hypothesized that the district court might hold that a BIPA violation occurs (1) “where the person whose privacy rights are impacted uses Facebook,” (2) “where Facebook scans photographs and

stores the templates,” or (3) “in some other place or combination of places.” *Id.* at 22. But regardless of the answer the district court ultimately chooses, the case will require mini-trials to determine if BIPA applies to each class member’s claims, creating individualized issues that will overwhelm common ones.

*First*, if the BIPA violation is deemed to occur when a person used Facebook in Illinois, each member of the class would, at the very least, need to establish that they used Facebook *in Illinois*. But the certified class is not limited to those people: it consists of all “Facebook users located in Illinois for whom Facebook created and stored a face template after June 7, 2011.” Op. 10. A class member located in Illinois who did not use Facebook in Illinois does not have a BIPA claim but is nonetheless a member of the certified class. Moreover, under *Avery*, BIPA should not apply to a person who fleetingly used Facebook in Illinois and neither uploaded photos of themselves from Illinois nor appeared in photos uploaded from Illinois. *See Avery*, 835 N.E.2d at 854 (Illinois law applies where the circumstances to a transaction occur “primarily and substantially in Illinois”). Thus, under the first scenario, class members would need to establish the nature, extent, and timing of relevant Facebook use in Illinois to bring a claim. These questions would easily and quickly overwhelm any questions common to the class.

The panel sidestepped this analysis by summarily observing that the district court had 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.” Op. 23 n.7. This ignored Facebook’s argument that nothing in the record indicates that class members used Facebook “mainly” in Illinois. And as the word “mainly” itself suggests, the district court’s vague conclusions about class members’ connections to Illinois merely highlight the need for mini-trials. If BIPA’s application turns on where someone “used Facebook,” then what matters is where, *specifically*, class members agreed to Facebook’s terms, where each one principally used Facebook, and where the photos of themselves that gave rise to the alleged BIPA violations were uploaded. *See, e.g., Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1102 (N.D. Ill. 2017) (in BIPA action involving facial recognition, holding that extraterritoriality doctrine turned on multiple factors, including the parties’ residency, where plaintiffs’ photos were uploaded, and where “the alleged scans actually t[ook] place”); *Monroy v. Shutterfly, Inc.*, No. 16-C-10984, 2017 WL 4099846, at \*6 (N.D. Ill. Sept. 15, 2017) (similar). These factors vary across the class and each class member will need to establish the factors relevant to their own claims to recover under BIPA.

*Second*, if the violation is deemed to occur where Facebook scans photos and stores face templates, then BIPA should not apply at all because the record shows that Facebook undertakes those activities wholly outside of Illinois. *See Graham v. Gen. U.S. Grant Post No. 2665, V. F. W.*, 248 N.E.2d 657, 659 (1969)

(Illinois law did not apply where the “necessary element of liability did not take place in Illinois”).

*Finally*, if the violation of BIPA is deemed to occur in a different location or a “combination of places,” the court would need to evaluate *all* of the *Avery* factors—both within and outside Illinois—to establish whether an individual class member’s alleged violation occurred “primarily and substantially” in Illinois. 835 N.E.2d at 854. For the same reasons, these individual questions would predominate over common ones.

**B. The Panel’s Opinion Extends BIPA Nationwide.**

The panel’s opinion presents another question of exceptional importance: whether a BIPA class action may be maintained against a service provider operating nationwide based on the mere allegation that class members are “located in” Illinois. This should not be enough for BIPA liability to attach, and to hold otherwise would effectively subject every online service provider in the country to the strictest and most punitive state law governing biometric technology.

The Dormant Commerce Clause of the U.S. Constitution prevents a state from “impos[ing] its own policy choice on neighboring States” or forcing foreign residents to live under its particular mandates. *BMW of N. Am., Inc. v. Gore*, 517 U.S. 559, 571 (1996). The “critical inquiry” under the clause “is whether the practical effect of [a state’s] regulation is to control conduct beyond the boundaries

of the State.” *Healy v. Beer Inst.*, 491 U.S. 324, 335-37 (1989). This Court recently reaffirmed this rule, concluding that a California statute violated the Dormant Commerce Clause where it attempted to regulate “sales that t[ook] place outside California” and had “no necessary connection with the state other than the residency of the seller.” *Sam Francis Found. v. Christies, Inc.*, 784 F.3d 1320, 1323 (9th Cir. 2015) (en banc). This doctrine reflects the “Constitution’s special concern both with the maintenance of a national economic union unfettered by state-imposed limitations on interstate commerce” and “with the autonomy of the individual States.” *Healy*, 491 U.S. at 335-37.

The panel’s conclusion that “there is no need to have mini-trials” on the issue of extraterritoriality raises serious questions under the Dormant Commerce Clause. It is a “cardinal principle” of statutory construction that “where an otherwise acceptable construction of a statute would raise serious constitutional problems, the court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress.” *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988).<sup>2</sup> Here, rather than evaluating whether each class member suffered a BIPA

---

<sup>2</sup> The Illinois Supreme Court applies the same principle to the interpretation of state statutes. *Wilson v. Dep’t of Revenue*, 169 Ill. 2d 306, 310 (1996) (courts “presume statutes to be constitutional and must construe enactments by the legislature so as to uphold their validity whenever it is reasonably possible to do so.”).

violation that occurred “primarily and substantially” in Illinois, thereby limiting the reach of BIPA to conduct within Illinois, the panel suggests—without actually deciding—that BIPA might reach conduct occurring wholly outside of Illinois. Under the panel’s reasoning, even though the class definition encompasses individuals “located in” Illinois who may never have used Facebook in that state, “mini-trials” are unnecessary to establish whether each class member is entitled to relief. Under this framework, even if most of the relevant conduct occurred outside Illinois, a class could be certified and the claim could proceed.

This failure to enforce the territorial limits of state law has serious consequences. Many states have chosen not to adopt Illinois’ strict approach to the regulation of biometric data, as is their right. *Mazza v. Am. Honda Motor Co., Inc.*, 666 F.3d 581, 591 (9th Cir. 2012) (“It is a principle of federalism that ‘each State may make its own reasoned judgment about what is permitted or proscribed within its borders.’”) (quoting *State Farm Mut. Auto Ins. Co. v. Campbell*, 538 U.S. 408, 422 (2003)). For example, California, where Facebook is headquartered, has chosen to regulate biometric information in an entirely different manner from Illinois—dispensing with the “informed written consent” requirement prior to collection, but granting to consumers other “rights” with respect to that data. *See* California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100, *et seq.* But the practical effect of the panel’s reasoning is that companies offering online

services will have to choose between complying with BIPA's requirements as to conduct occurring wholly outside Illinois, or risk BIPA class actions with damages exposure that may pose existential threats.

It is no answer to say that companies can simply comply with Illinois law in Illinois and comply with other states' laws elsewhere. Companies that offer online services cannot always perfectly determine whether someone using their services is "in Illinois." While some methods to estimate users' locations may be available, they are imperfect and often approximate or incomplete. For example, people can limit or disguise the location information they share with online providers, further complicating any effort to target compliance measures to a particular state. They can choose not to share location information through their phones, or they may choose to not use phones at all and rely instead on desktop computers, which generally do not share GPS data. They can use virtual private networks (VPNs) that pass all network traffic through a single IP address, they can spoof their IP address to make it look like they are in a different state or country, or they can use anonymity networks to hide their location.

In addition, requiring companies to ascertain and track users' locations, even when such data is not necessary or useful to provide or improve the companies' services, could undermine users' privacy interests—precisely the opposite of what BIPA intended.

Over 300 BIPA class actions have been filed to date, many against companies that operate nationwide. To avoid liability under BIPA and ensure that all individuals within Illinois are covered, online companies will almost certainly need to be over-inclusive—applying BIPA to services offered outside Illinois. And if a BIPA class can be certified, and the cudgel of classwide statutory damages can be wielded based on nothing more than someone’s location in Illinois, then those companies will have no choice but to assume that everyone is a potential BIPA plaintiff. That outcome would harm not only technology companies, but also the millions of users of their products who would lose access to features they enjoy. Rehearing should be granted so that this Court can avoid those consequences by enforcing the constitutional limits on the scope of BIPA.

**II. VITIATING ARTICLE III STANDING REQUIREMENTS WOULD HAVE A SUBSTANTIAL AND DELETERIOUS IMPACT ON THE ASSOCIATION’S MEMBERS.**

The panel determined that plaintiffs, despite suffering no injury other than an alleged violation of BIPA’s notice-and-consent requirements, suffered a concrete injury for purposes of Article III standing. Op. 17. But allowing litigants to access federal courts based on nothing more than a claimed violation of a state statute risks opening a floodgate to “gotcha” class actions that offer no benefit to the public and instead stifle technology by making useful features and products more costly.

This concern is not hypothetical. The list of companies sued for BIPA violations without a showing of actual harm is long and growing. It includes not only many of the world's most renowned companies<sup>3</sup> but also dozens of small- and medium-sized businesses that have less name recognition and fewer means to defend themselves against these costly lawsuits. Allowing class actions to proceed without a showing of harm would upend the balance struck by the legislature and turn BIPA into a vehicle for extracting outsized settlements. Without an injury requirement, there is no barrier to filing cookie-cutter class actions motivated mainly by the prospect of a massive award under BIPA's statutory damages provisions. Indeed, BIPA class actions have been filed principally by the same handful of law firms.

---

<sup>3</sup> This list includes: Amazon (feature that allows Alexa to recognize voices); American Airlines (finger scan-based timekeeping for employees); Dr. Pepper/Seven Up (finger scan-based timekeeping for employees); Google (photo storage feature that allows users to search by face and feature that allows Google Assistant to interpret speech); H&M (finger scan-based timekeeping for employees); Harbor Freight Tools (finger scan-based technology of individuals at store locations); Home Depot (use of facial recognition cameras for security purposes in stores); Hyatt hotels (finger scan-based timekeeping for employees); McDonald's restaurants (same); Roundy's supermarkets (same); Shutterfly (photo storage feature that allows users to search by face); Six Flags (finger scan equipment to enter amusement park); Southwest Airlines (finger scan-based technology timekeeping for employees); Universal Parks & Resorts (finger scan equipment to enter amusement park); Symphony Healthcare (finger scan-based timekeeping for employees); Walmart (hand scan for using cash register); and White Castle Foods (finger scan-based timekeeping for employees). These are just a small fraction of the over 300 companies sued under BIPA based on an alleged bare statutory violation since 2015.

The threat of staggering damages awards through no-harm class actions would deter innovation—an outcome that the Illinois legislature sought to avoid. Consumers appreciate, enjoy, and increasingly expect features like voice and face recognition in the products and services they use. Consumers use these technologies out of convenience, such as to avoid having to remember passwords or carry keys and badges. They also opt for biometric authentication technologies where security is of heightened concern—for example, in online banking. PR Newswire, *IBM Future of Identity Study: Millennials Poised to Disrupt Authentication Landscape* (Jan. 29, 2018), <https://www.prnewswire.com/news-releases/ibm-future-of-identity-study-millennials-poised-to-disrupt-authentication-landscape-300589262.html> (finding a plurality of respondents ranked fingerprint biometrics as the most secure method of authentication).

Biometric technology is also socially beneficial. As the Illinois legislature recognized, it “promise[s] streamlined financial transactions and security screenings.” 740 Ill. Comp. Stat. 14/5(a). On the one hand, it offers consumers and businesses both improved security and increased convenience, *see, e.g.*, Stephan Rabimov, *Evolution on Lock: From Stick to Gate*, *Forbes* (Dec. 27, 2017, 5:42 PM); protects against gun violence, *see, e.g.*, Don Reisinger, *How Technology May Make Guns Safer*, *Fortune* (Dec. 3, 2015); keeps students safe in school through secure checkpoints and helps track their class attendance, Emily Ann Brown,

*Benefits of Biometrics* (Mar. 19, 2019), District Administration, <https://districtadministration.com/biometric-security-boosts-school-safety-efficiency/>; and facilitates social activities like organizing and sharing photos, as Facebook’s technology did in this case.

On the other hand, the security risk flowing from collection and storage of biometric data is not as dire as the panel imagines. Most biometric data are not only converted to a proprietary code but also encrypted or hashed, so in most cases a breach of biometric data would reveal encrypted gibberish that nobody could understand. *See supra Benefits of Biometrics* (explaining how a particular finger scanner “identif[ies] into hundreds of unique swirls, ridges and points on a . . . finger and translate[d] . . . into a binary number [that is] encrypted . . . [so that] none of the scans can be recreated”); *See also* Wash. Rev. Code 19.375.010(5) (recognizing that biometric identifiers are typically “convert[ed] . . . into a reference template that cannot be reconstructed into the original output image”). The potential downside of a security breach thus tends to be lower with respect to biometric data than with other types of personal information, which are less likely to be secured through measures like encryption.

Certifying a class under BIPA without the rigorous application of Article III standing rules risks imperiling not just social and entertainment uses of biometrics, but also uses that protect people, such as security cameras that can recognize

strangers outside the home, fingerprint readers that prevent access to sensitive information, and facial recognition systems that can help locate missing children. This Court should not undermine these promising technologies by opening the Ninth Circuit courts to opportunistic lawsuits based on bare statutory violations of the nation's strictest biometric privacy law. Instead, it should grant en banc review of the panel's decision so that it can enforce the Article III precedent of this Court and the U.S. Supreme Court.

### **CONCLUSION**

For the foregoing reasons, as well as the reasons in the Defendant-Appellant's petition, the Court should grant rehearing en banc.

Respectfully submitted,

/s/ Susan Fahringer

Susan D. Fahringer  
Nicola C. Menaldo  
Ryan Spear  
PERKINS COIE LLP  
1201 Third Avenue, Suite 4900  
Seattle, WA 98101  
Telephone: (206) 359-8000  
sfahringer@perkinscoie.com  
nmenaldo@perkinscoie.com  
rspear@perkinscoie.com

Sunita Bali  
PERKINS COIE LLP  
505 Howard Street, Suite 1000  
Telephone: (415) 344-7000  
San Francisco, CA 94105  
sbali@perkinscoie.com

*Counsel for Amicus Curiae Internet  
Association*

September 16, 2019

UNITED STATES COURT OF APPEALS  
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: <http://www.ca9.uscourts.gov/forms/form08instructions.pdf>

9th Cir. Case Number(s)

I am the attorney or self-represented party.

This brief contains  words, excluding the items exempted

by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief (*select only one*):

- complies with the word limit of Cir. R. 32-1.
- is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- complies with the longer length limit permitted by Cir. R. 32-2(b) because (*select only one*):
  - it is a joint brief submitted by separately represented parties;
  - a party or parties are filing a single brief in response to multiple briefs; or
  - a party or parties are filing a single brief in response to a longer joint brief.
- complies with the length limit designated by court order dated .
- is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature

Date

(use "s/[typed name]" to sign electronically-filed documents)

Feedback or questions about this form? Email us at [forms@ca9.uscourts.gov](mailto:forms@ca9.uscourts.gov)

### **CERTIFICATE OF SERVICE**

I certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on September 16, 2019. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

/s/ Susan D. Fahringer  
Susan D. Fahringer