Golden Gate University Law Review

Volume 50
Issue 1 *Ninth Circuit Survey*

Article 9

June 2020

Patel v. Facebook, Inc.: The Collection, Storage, and Use of Biometric Data as a Concrete Injury under BIPA

Jessica Robles
Golden Gate University School of Law

CASE SUMMARY

PATEL V. FACEBOOK, INC.: THE COLLECTION, STORAGE, AND USE OF BIOMETRIC DATA AS A CONCRETE INJURY UNDER BIPA

*JESSICA ROBLES**

INTRODUCTION

Facebook, Inc. ("Facebook") amassed one of the most extensive facial-template databases in the world through the use of facial-recognition technology.[1] However, Facebook is not alone; both private and public sector entities are heavily investing in improving their facial-identification technology.[2] Facial geometry data are unique to each person[3] and can be used to identify an individual. Once a facial image has been captured and stored in a facial-template database, "the individual has no recourse" because one cannot change facial geometry as quickly as a password or a social security number.[4]

Although companies may use facial-recognition technology for valid purposes, uses of facial-recognition technology to target specific groups raise "questions around abuse, consent, weaponization, and discrimina-

* J.D. Candidate, 2020, Golden Gate University School of Law; B.A. Mathematics, California State University, San Bernardino; Associate Editor, *Golden Gate University Law Review*.

[1] Cade Metz, *Facial Recognition Tech Is Growing Stronger, Thanks to Your Face*, N.Y. TIMES (July 13, 2019), https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html.

[2] Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, AM. BAR ASS'N, https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/ (last visited Sept. 30, 2019).

[3] Cade Metz, *Facial Recognition Tech Is Growing Stronger, Thanks to Your Face*, N.Y. TIMES (July 13, 2019), https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html.

[4] Patel v. Facebook, Inc., 932 F.3d 1264, 1269 (2019) (quoting the Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/5(c) (2008) (internal quotation marks omitted)).

tory uses of this technology."[5] From a privacy standpoint, the potential use of facial-recognition technology to search against millions of photographs without the consent of "law-abiding citizens is a major privacy violation."[6] These concerns have fueled an increase in data privacy legislation[7] as well as litigation, such as *Patel v. Facebook, Inc*.

I. BACKGROUND

Both private sector and public sector facial identification databases put individuals at risk of mistaken identity, unauthorized searches, and erosion of due-process protections.[8] With these risks in mind, a few states enacted biometric privacy statutes.[9] In 2008, the Illinois General Assembly passed the Illinois Biometric Information Privacy Act ("BIPA") to regulate the use of biometric identifiers.[10] BIPA is unique because it provides for a private right of action, meaning that Illinois residents can file a lawsuit seeking damages for violations of the statute.[11] This contrasts with the laws in other states, which only allow state actors to bring claims on behalf of private individuals. Allowance of a private cause of action has generated a multitude of lawsuits.[12] Two re-

[5] Kate Kaye, *This Little-Known Facial-Recognition Accuracy Test Has Big Influence*, INT'L ASS'N OF PRIVACY PROF'LS (Jan. 7, 2019), https://iapp.org/news/a/this-little-known-facial-recognition-accuracy-test-has-big-influence/ (quoting Joy Buolamwini (internal quotations omitted)).

[6] Catie Edmondson, *ICE Used Facial Recognition to Mine State Driver's License Databases*, N.Y. TIMES (July 7, 2019), https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html?module=inline; *see also* Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, WASH. POST. (July 7, 2019 12:54 p.m.), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

[7] *Consumer Data Privacy Legislation*, NAT'L CONFERENCE OF STATE LEGISLATURES (Oct. 14, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.

[8] Nicole Black, *Who Stole My Face? The Risks of Law Enforcement Use of Facial Recognition Software*, ABOVE THE LAW (Nov. 14, 2019), https://abovethelaw.com/2019/11/who-stole-my-face-the-risks-of-law-enforcement-use-of-facial-recognition-software/.

[9] Molly K. McGinley, Kenn Brotman, Erinn L. Rigney, *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States*, NAT'L L. REV. (Mar. 25, 2019), https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states.

[10] Biometric Information Privacy Act, 740 ILL. COMP. STAT. §§ 14/1-14/99 (2008).

[11] Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/20 (2008).

[12] *See, e.g.* Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1207 (Ill. 2019) (finding Article III standing where defendant failed to provide notice or obtain written consent for the collection, storage, and use of a fourteen year old's fingerprint). *But see* Santana v. Take-Two Interactive Software, Inc., 717 Fed.App'x. 12, 16-17 (2d Cir. 2017) (finding no Article III standing where defendant informed users that a face scan used to create a gaming avatar would be visible to other players); Rivera v. Google, 366 F. Supp. 3d 998, 1007-11 (N.D. Ill. Dec. 29, 2018) (finding no Article III standing where plaintiffs failed to provide evidence that the collection of facial scans created a substantial risk of identity theft); McCollough v. Smarte Carte, Inc., No. 16C03777, 2016

cent cases finding Article III standing are *Rosenbach v. Six Flags Entertainment Corp.* and *Patel v. Facebook, Inc.*

Private individuals who bring a claim under BIPA must still have standing to sue. To have standing to sue, the plaintiff must allege an injury-in-fact that is fairly traceable to the defendant's conduct, and that the injury is likely to be redressed by a favorable judicial opinion.[13] In *Rosenbach*, the Illinois Supreme Court defined an injury-in-fact by holding that "in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to [BIPA]," the individual does not need to claim a harm "beyond [a procedural] violation of his or her rights under [BIPA]."[14] In *Patel*, the United States Court of Appeals for the Ninth Circuit ("Ninth Circuit") echoed the Illinois Supreme court's decision in *Rosenbach* by reaffirming that, for purposes of establishing standing in the federal courts, a violation of intangible statutory rights under BIPA without further harm is a sufficient injury-in-fact.[15] Moreover, in *Patel*, the Ninth Circuit applied this definition of an injury-in-fact to affirm the district court's class certification and denial of a motion to dismiss for lack of standing.[16]

A. FACTUAL BACKGROUND

Facebook is a social networking company with over two billion active users worldwide.[17] New users register, create a user profile, may add friends, and interact with their network by sharing content.[18] In 2010, Facebook launched its tag suggestions program.[19] The tag suggestions program uses facial-recognition technology to scan the photographs that users upload to suggest to the user to tag a specific person.[20]

When a user creates a profile and adds a picture of one's face, Facebook gathers information from the image and creates a face tem-

---

U.S. Dist. LEXIS 100404 (N.D. Ill. Aug. 1, 2016) (finding no Article III standing where defendants failed to notify or obtain consent prior to scanning fingerprints used to lock and unlock storage lockers).

[13] Patel v. Facebook Inc., 290 F. Supp. 3d 948, 952 (N.D. Cal. 2018).

[14] Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1207 (Ill. 2019).

[15] *See* Patel v. Facebook, Inc., 932 F.3d 1264, 1274 (9th Cir. 2019).

[16] *See Id*.

[17] J. Clement, *Number of Facebook Users Worldwide 2008-2019*, STATISTA (Aug. 9, 2019), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (last visited Sept. 27, 2019).

[18] J. Clement, *Number of Facebook Users Worldwide 2008-2019*, STATISTA (Aug. 9, 2019), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (last visited Sept. 27, 2019).

[19] *Facebook*, 932 F.3d at 1268.

[20] *Id*.

plate.[21] Facebook stores face templates in one of its data centers,[22] many of which are located in the United States.[23] When a second user uploads a picture, the facial-recognition technology gathers "various geometric data points" from that image and generates a facial map or "signature."[24] Under BIPA, a person's facial signature or facial geometry, is a biometric identifier.[25] The technology then runs these new facial signatures against its large database of face templates to determine whether the face signature matches a face template already in the database.[26] If there is a match, Facebook then suggests the second user tag the person in the image who matches a face template.[27]

B. PROCEDURAL BACKGROUND

Plaintiffs Carlo Licata, Nimesh Patel, and Adam Penzen, sued Facebook in separate lawsuits for BIPA violations.[28] In August 2015, the plaintiffs consolidated their separate lawsuits into a class action complaint and became class representatives.[29] The Illinois plaintiffs alleged that the tag suggestions program violated sections 15(a) and 15(b) of BIPA because Facebook failed to provide notice and obtain written consent before generating, storing, and using their biometric identifiers.[30]

On February 26, 2018, the district court denied a motion to dismiss for lack of standing.[31] The district court held that a transgression of the BIPA notice and consent provisions "is an intangible harm that constitutes a concrete injury-in-fact."[32] Two months later, on April 16, 2018, the district court certified the class consisting of "Facebook users located in Illinois for whom Facebook created and stored a face template after June 7, 2011."[33] Facebook then appealed the district court's ruling.[34]

---

[21] *Id*.

[22] *Id*.

[23] Rachel Peterson, *Data Centers Year in Review*, FACEBOOK ENG'G (Jan. 1, 2019), https://engineering.fb.com/data-center-engineering/data-centers-2018/.

[24] *Facebook*, 932 F.3d at 1268.

[25] Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/10 (2008).

[26] *Facebook*, 932 F.3d at 1268.

[27] *Id*. at 1268.

[28] *Facebook*, 290 F. Supp. 3d at 950–51.

[29] *See Facebook*, 932 F.3d at 1268; *see also In re* Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1159 (N.D. Cal. 2016).

[30] *Facebook,* 932 F.3d at 1268; *Facebook*, 290 F. Supp. 3d at 951.

[31] *Facebook*, 290 F. Supp. 3d at 950.

[32] *Id*. at 954.

[33] *In re Facebook*, 326 F.R.D. at 540.

[34] *Facebook*, 932 F.3d at 1269–70.

II. NINTH CIRCUIT ANALYSIS

A. ARTICLE III STANDING TWO-STEP APPROACH

The Ninth Circuit began its analysis by determining whether the plaintiffs had standing.[35] The court explained that to establish Article III standing, a plaintiff must have suffered an injury-in-fact.[36] To establish an injury-in-fact, the court must find that the harm to the plaintiff is concrete and particularized, and actual or imminent.[37] The Ninth Circuit clarified that even an intangible injury might qualify as an injury-in-fact as long as it is sufficiently concrete.[38] To determine whether an injury is sufficiently concrete, the court considers history and legislative intent.[39]

Similar to the district court, the Ninth Circuit used a traditional two-step approach to determine whether the statutory violation caused a concrete injury.[40] Under the test, a court asks (1) whether "the statutory provisions at issue were established to protect the plaintiff's concrete interests, 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."[41] The Ninth Circuit then applied each part of the test.

1. The Capture and Use of Biometric Information Without Consent Invades Concrete Interests

Facebook contended that their alleged non-compliance with BIPA's notice and consent provisions amounted to a procedural violation of BIPA without actual harm to the plaintiffs.[42] Moreover, Facebook argued that a statutory violation of BIPA was insufficient to establish a concrete injury for purposes of Article III standing.[43] The plaintiffs argued that under BIPA, they suffered a concrete injury when Facebook generated, stored, and used their facial geometries without their consent.[44] Addi-

---

[35] *Facebook*, 932 F.3d at 1270.

[36] *Id*.

[37] *Id*. (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992) (internal quotations omitted)).

[38] *Id*.

[39] *Id*. (quoting Robins v. Spokeo, Inc., 867 F.3d 1108, 1113 (9th Cir. 2017) (internal quotations omitted)).

[40] *Id*. at 1270–71.

[41] *Id*. (quoting *Spokeo*, 867 F.3d at 1113 (internal quotations omitted)).

[42] *Id*. at 1271.

[43] *Id*. at 1271.

[44] *Id*. at 1271.

tionally, the plaintiffs stated that a procedural violation is a concrete injury, and that they did not have to claim additional harms.[45]

To determine whether a concrete interest existed, the Ninth Circuit first looked to history to assess whether the alleged privacy harm resembled one that provided grounds for a lawsuit in the past.[46] The court found that the Supreme Court of the United States had recognized that a right to privacy existed at common law stemming from both tort law and constitutional law.[47] Moreover, the court stated that the majority of American jurisdictions have recognized the existence of a right to privacy and that many states have actions to remedy privacy torts.[48] Additionally, the court explained that the Supreme Court of the United States has considered how new technology intrudes on the right of privacy in its Fourth Amendment jurisprudence.[49] The Ninth Circuit concluded that a violation 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."[50]

The Ninth Circuit explained that the common law understanding of privacy includes the "individual's control of information concerning his or her person."[51] The court stated that, similar to the cell-site location technology in *Carpenter v. United States*,[52] facial-recognition technology could gather highly-detailed information.[53] The detailed information could be used to identify an individual in any of the millions of photographs uploaded to Facebook and to pinpoint the individual's location.[54] The court also looked to future uses of facial-recognition technology such as to identify the individual from a street surveillance photograph or to unlock their cell phone.[55] Hence, the creation of a face template using facial-recognition technology without consent and without alleging further harm infringes on concrete interests.[56]

---

[45] *See id*.

[46] *Id*. at 1271–72 (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) (internal quotation marks omitted)).

[47] *Id*. at 1271–73.

[48] *Id*. at 1272.

[49] *See id*. 1272–73; Kyllo v. U.S., 533 U.S. 27, 34 (2001) (involving thermal imaging); U.S. v. Jones, 565 U.S. 400, 416 (2012) (involving GPS); Carpenter v. U.S., 138 S. Ct. 2206, 2215 (2018) (involving cell-site location information); Riley v. CA, 573 U.S. 373, 386 (2014) (involving cell phone storage).

[50] *Id*. at 1273 (quoting *Spokeo*, 136 S. Ct. At 1549 (internal quotation marks omitted)).

[51] *Id*. (quoting U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 763 (1989) (internal quotation marks omitted)).

[52] *Carpenter*, 138 S. Ct. 2206.

[53] *Facebook*, 932 F.3d at 1273.

[54] *Id*. at 1273.

[55] *Id*.

[56] *Id*.

Next, the Ninth Circuit examined legislative judgment. The court observed that the Illinois General Assembly stated that "[t]he public welfare, security, and safety will be served by regulating" the collection, storage, use, and deletion or biometric information.[57] Moreover, the court found that BIPA was enacted to protect an individual's privacy rights in their biometric identifiers.[58] The Ninth Circuit agreed with the Illinois Supreme court that a person "could be 'aggrieved' . . . whenever a private entity fails to comply" with section 15 of BIPA.[59] The Ninth Circuit concluded that section 15 of BIPA was designed to protect concrete interests.[60]

2. *The Collection, Storage, and Use of Plaintiffs' Face Templates Is A Substantive Harm*

The plaintiffs contended that the collection, use, and storage of their face templates without consent violated section 15(b) of BIPA and that they did not need to claim further harms.[61] Facebook argued that plaintiffs needed to claim harm beyond a procedural violation and relied on *Bassett v. ABM Parking Services*.[62] In *Bassett*, the defendant violated the Fair Credit Reporting Act by not redacting a credit card's expiration date on a receipt.[63] The *Bassett* court did not find a substantive harm because the violation did not cause a disclosure of the consumer's financial information.[64]

The Ninth Circuit stated that under the common law, an intrusion into privacy rights by itself makes a defendant subject to liability.[65] The court explained that the protected privacy right "is the right not to be subject to the collection and use of such biometric data . . . ."[66] Furthermore, the Ninth Circuit distinguished *Bassett* because the Fair Credit Reporting Act was designed to prevent disclosure and identity theft.[67] In *Bassett*, Congress specified in amendments to the Fair Credit Reporting Act that to establish a willful violation of the statute requires an allega-

---

[57] *Id*. (quoting Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/5(g) (2008) (internal quotations omitted)).

[58] *Id*.

[59] *Id*. at 1274 (quoting Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1206 (Ill. 2019)).

[60] *Id*.

[61] *Id*.

[62] *Id*. at 1271; Bassett v. ABM Parking Servs., 883 F.3d 776 (9th Cir. 2018).

[63] *Facebook*, 932 F.3d at 1274.

[64] *Id*.

[65] *Id*.

[66] *Id*.

[67] *Bassett*, 883 F.3d 776.

tion of harm to the consumer's identity.[68] BIPA does not require a further allegation of disclosure or harm.[69]

Thus, under BIPA, the mere collection and use of biometric data without consent "would necessarily violate the plaintiffs' substantive privacy interests."[70] Since both parts of the two-step approach were met, the Ninth Circuit held that the plaintiffs alleged a concrete and particularized harm, sufficient to establish Article III standing.[71]

B. THE DISTRICT COURT DID NOT ABUSE ITS DISCRETION IN GRANTING CLASS CERTIFICATION

The general standard of review when parties appeal from the grant of class certification is "abuse of discretion."[72] The district court is given more deference when reviewing a grant of class certification than when reviewing a denial.[73] A district court abuses its discretion when it makes an error of law.[74] The court had to review de novo the legal determinations made in support of the decision to grant class certification.[75]

Facebook argued that the district court abused its discretion by granting class certification.[76] First, Facebook claimed that questions of law or fact common to class members did not predominate over questions affecting individual plaintiffs.[77] Second, Facebook contended that the potential for a significant statutory damages award would make individual actions superior to the difficulties of managing a class action lawsuit.[78]

3. Questions of Law or Fact Common to Class Members Predominate

Facebook argued that questions of law or fact common to class members did not predominate over questions affecting individual plaintiffs.[79] Facebook contended that BIPA violations can occur in several

---

[68] *See Bassett*, 883 F.3d at 778.

[69] *See Facebook*, 932 F.3d at 1275.

[70] *Id*. at 1274.

[71] *Id*. at 1275.

[72] *Id*.

[73] *Id*. (quoting Just Film, Inc. v. Buono, 847 F.3d 1108, 1115 (9th Cir. 2017) (internal quotations omitted)).

[74] *Id*. (quoting Sali v. Corona Reg'l Med. Ctr., 909 F.3d 996, 1002 (9th Cir. 2018)).

[75] *Id*.

[76] *Id*.

[77] *Id*. at 1276.

[78] *Id*. (citing FED. R. CIV. P. 23(b)(3)).

[79] *Id*.

locations, such as where: the person uses Facebook, Facebook scans photographs, or Facebook stores face templates.[80] Using the Illinois extraterritoriality doctrine, Facebook believed that each plaintiff must provide evidence that events in their case occurred primarily and substantially within the state of Illinois.[81] Facebook suggested that class members provide individualized proof of the location where relevant events transpired.[82] Relevant events would include where: the photograph was uploaded, Facebook performed facial recognition analysis, or Facebook gave a tag suggestion.[83] Thus, according to Facebook, questions individual to each class member would predominate.[84]

The court stated that there was predominance sufficient for class certification when "questions of law or fact common to class members predominate over any questions affecting only individual members."[85] Moreover, under the Illinois extraterritoriality doctrine, an Illinois plaintiff may not maintain a cause of action under a state statute for transactions that transpired outside of Illinois.[86] However, plaintiffs can bring an action if the events of the transaction occurred "primarily and substantially within Illinois."[87]

The Ninth Circuit expressed that extraterritoriality questions could be decided on a class-wide basis without defeating predominance.[88] The questions created by the extraterritoriality doctrine included whether relevant events took place primarily and substantially in Illinois, or outside of Illinois.[89] Additionally, the court determined that the Illinois General Assembly intended that BIPA apply to "individuals who are located in Illinois, even if some relevant activities occur outside the state."[90] Thus, the court found that the district court did not err in finding predominance.[91] Next, the court analyzed whether the lower court erred by finding superiority.

---

[80] *Id*. at 1275.

[81] *Id*.

[82] *Id*.

[83] *Id*.

[84] *Id*. at 1275–76.

[85] FED. R. CIV. P. 23(b)(3).

[86] *Id*. at 1275 (citing Avery v. State Farm Mut. Auto. Ins. Co., 835 N.E.2d 801, 853 (Ill. 2005)).

[87] *Id*. (quoting *Avery*, 835 N.E.2d at 853–54 (internal quotation marks omitted)).

[88] *Id*. at 1276.

[89] *Id*.

[90] *Id*.

[91] *See id*.

4. The Potential for Significant Statutory Damages Does Not Make Individual Actions Superior to a Class Action Lawsuit

Facebook contended that individual lawsuits would be superior because it would be difficult to manage such a large class action.[92] Additionally, Facebook claimed that individual actions would be superior to a class action because of the potential for a significant statutory damages award.[93] BIPA allows for damages of one thousand dollars for each negligent violation, or five thousand dollars for each intentional or reckless violation.[94]

The court explained that there is superiority sufficient for class certification when the class action is "superior to other available methods for fairly and efficiently adjudicating the controversy."[95] The court responded to Facebook's argument by clarifying that the issue of caps on statutory damages depends on the intent of the legislature, which the court gathers from the express statutory language and legislative history.[96] The court explained that BIPA's text and legislative history did not cap statutory damages.[97] Moreover, the text and legislative history did not indicate that substantial statutory damages were contrary to the intent of the Illinois General Assembly.[98] Therefore, the court affirmed the district court's ruling and added that there was no error of law or abuse of discretion in granting class certification.[99]

III. IMPLICATIONS OF PATEL V. FACEBOOK, INC.

Following the Ninth Circuit's opinion, on October 18, 2019, the court denied a petition for rehearing en banc.[100] On October 30, 2019, the court granted a motion to stay while Facebook petitions for writ of certiorari in the Supreme Court of the United States.[101] A Supreme Court of the United States' decision could resolve the current circuit split and

---

[92] *See id*. (citing FED. R. CIV. P. 23(b)(3)).

[93] *Id*. (citing FED. R. CIV. P. 23(b)(3)).

[94] Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/20 (2008).

[95] *Id*. (quoting FED. R. CIV. P. 23(b)(3)(D)).

[96] *Id*. 1276.

[97] *See id*. at 1277.

[98] *Id*.

[99] *Id*. at 1276–77.

[100] Josh Constine, *$35B Face Data Lawsuit Against Facebook Will Proceed*, TECH CRUNCH (Oct. 18, 2019), https://techcrunch.com/2019/10/18/facebook-35-billion-lawsuit/.

[101] Daniel R. Stoller, *Facebook Biometric Case Halted Pending Supreme Court Appeal*, BLOOMBERG LAW (Oct. 31, 2019, 7:17 AM), https://news.bloomberglaw.com/privacy-and-data-security/facebook-biometric-case-halted-pending-supreme-court-appeal.

clarify which intangible privacy harms are sufficient to bring a claim in federal court.[102]

The increasing number of privacy-related lawsuits and government fines reflect society's growing concern that emerging technologies' ability to collect detailed personal information can negatively impact individuals now and in the future. In addition to lawsuits brought by plaintiffs, government agencies have enforced fines on technology companies for privacy violations.[103] For example, in July 2019, the Federal Trade Commission and Facebook announced a five billion dollar settlement for privacy-related violations.[104]

On September 3, 2019, a month after the Ninth Circuit's decision, Facebook responded by changing its tag suggestions program from a default setting of on with an opt-out option to a default setting of off with an opt-in option.[105] Facebook's modifications to its tag suggestion program following the court's opinion indicate that both litigation and government fines are helping to enforce higher data privacy standards. Fears of similar litigation and penalties for privacy violations will motivate other companies to evaluate their use of data to comply with existing privacy laws and future legislation.[106]

CONCLUSION

The Ninth Circuit's decision affirmed the district court's denial of a motion to dismiss for lack of standing and affirmed the class certification.[107] This case reinforces that an intangible injury such as the collection, storage, and use of biometric data without consent can be sufficient to constitute a concrete injury-in-fact to confer Article III standing.[108] If the United States Supreme Court denies Facebook's petition for certio-

---

[102] *Id*.

[103] Jay Cline, *U.S. Takes The Gold in Doling Out Privacy Fines*, COMPUTERWORLD (Feb. 17, 2014), https://www.computerworld.com/article/2487796/jay-cline—u-s—takes-the-gold-in-doling-out-privacy-fines.html.

[104] *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[105] Srinivas Narayanan, *An Update About Face Recognition on Facebook*, FACEBOOK NEWSROOM (Sept. 3, 2019), https://newsroom.fb.com/news/2019/09/update-face-recognition/.

[106] *Consumer Data Privacy Legislation*, NAT'L CONFERENCE OF STATE LEGISLATURES (Oct. 14, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.

[107] *See Facebook*, 290 F. Supp. 3d at 956; *see also In re Facebook*, 326 F.R.D.

[108] *Facebook*, 932 F.3d at 1270 (citing *Spokeo*, 136 S. Ct. at 1549 (2016)).

rari, the underlying class action will continue to trial in the district court, where Facebook stands to lose billions of dollars in damages.[109]

[109] Josh Constine, *$35B Face Data Lawsuit Against Facebook Will Proceed*, TECH CRUNCH (Oct. 18, 2019), https://techcrunch.com/2019/10/18/facebook-35-billion-lawsuit/.