*Gonzalo Pereda*

**Case title:** “Patel v. Facebook, Inc”.

**Case Summary and Outcome**

The United States (U.S.) Court of Appeals for the District of California Circuit ruled that the breach of the Biometric Information Protection Act (BIPA) by Facebook posed a concrete harm to the privacy interests of its users and therefore allowed access to sue for compensation. A group of Facebook users filed a complaint against the social media platform on the ground that its facial recognition technology, which collects, stores, and uses biometric identifiers and biometric information, violated certain sections of BIPA, and so injured their right to privacy. They argued that Facebook obtained their biometric identifiers from the photos they uploaded on the platform without first obtaining a written release and lacking a compliant retention schedule. Facebook argued that this was a mere procedural violation that constituted no real injury to its users. The Court ruled that the failure of Facebook to comply with BIPA’s procedures constituted a material risk of harm to the privacy interests of its users. This means that the infringement of BIPA’s procedural provisions by private entities generates an intangible harm that allows individuals to sue for compensation.

**Facts**

Illinois’s citizens Adam Pezen, Nimesh Patel, and Carlo Licata are Facebook users since 2005, 2008, and 2009 respectively. In 2010 Facebook introduced facial recognition technology through a feature called Tag Suggestions. In essence, this technology enables Facebook to scan its users’ photos to create face signatures with their biometric identifiers. Facebook uses that biometric information to compare the face signature with its photo database and make tagging suggestions to users.

The three plaintiffs filed a class action complaint in a California district court in 2015 on the grounds that Facebook had breached sections 15(a) and 15(b) of the Biometric Information Protection Act by collecting, using, and storing biometric identifiers from their photos without obtaining a written release and without a compliant retention schedule [p. 7]. Section 15(a) states that “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”, while Section 15(b) states that “no private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first receives a written release executed by the subject of the biometric identifier or biometric information”.

Under the American common law system, courts adjudicate cases and not hypothetical disputes. In consequence, to file a claim before court plaintiffs must ascertain a concrete injury in fact due to the violation of a right created by a statute. In other words, to meet the irreducible constitutional minimum of Article III standing and file a lawsuit, plaintiffs must allege an injury that is concrete and particularized. Failing to prove an actual or imminent invasion of a legally protected interest results in a lack of standing and a dismissal of the case. *Lujan v. Defs. Of Wildlife, 504 U.S. 555, 560-561 (1992).* Facebook argued that the breach of a mere procedural violation of BIPA did not entail a concrete injury to the plaintiffs’ privacy rights and therefore failed to confer Article III standing. Plaintiffs, in turn, argued 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 [p. 13].

In June 2016, the district court denied Facebook’s motion to dismiss the plaintiffs’ complaint for lack of Article III standing. Additionally, the court 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” [p. 10]. The district court’s ruling was appealed by the defendant. In August 2018 the Court of Appeals reviewed (i) the district court’s order granting class certification and (ii) if the plaintiffs had Article III standing [p. 10].

**Decision overview**

Judge Ikuta delivered the judgment of the Court of Appeals for the 9th Circuit of California, United States.

The main issue before the Court was whether the failure of Facebook to comply with the procedures established in BIPA constitutes an injury in fact, i.e. an invasion of a legally protected interest that is concrete and particularized, and actual or imminent, that gives users Article III standing to file a complaint before court, *Lujan v. Defs. Of Wildlife, 504 U.S. 555, 560-561 (1992)*. Put in other words, ¿Does a statutory violation by Facebook constitute a concrete injury to its users’ privacy rights susceptible to generate liability? ¿Does the collecting, using, and storing of biometric information without a written release allow users to file for compensation?

Plaintiffs [argued](https://epic.org/amicus/bipa/patel-v-facebook/Patel-v-FB-Consolidated-Class-Action-Complaint.pdf) that Facebook systematically and automatically collected, used, and stored their biometric identifiers without complying with BIPA’s procedural regulations. They affirmed that this violated their substantive rights to privacy as set forth in BIPA and constituted a concrete injury. On the contrary, Facebook [argued](https://epic.org/amicus/bipa/patel-v-facebook/Patel-v-FB-9th-Cir-Redacted-Opening-Brief-Public.pdf) that plaintiffs suffered no real harm from its procedural violation of BIPA. Therefore, the failure to demonstrate real and concrete injury, monetary, emotional, reputational, or otherwise, results in a lack of Article III standing, because plaintiffs had not been harmed by Facebook’s alleged conduct.

BIPA was enacted by the Illinois General Assembly in 2008 to serve the public welfare, security, and safety “by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information”. 740 Ill. Comp. Stat. 14/5(g). BIPA’s definition of “Biometric identifier” includes “the retina or iris scan, (…) scan of hand or face geometry”; it also defines “Biometric information” as “any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual”. 740 Ill. Comp. Stat. 14/10. BIPA gives a right of action to any person aggrieved by a violation of the Act. 740 Ill. Comp. Stat. 14/20. As stated under “Facts”, relevant provisions are Section 15(a), which states that “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”, and Section 15(b), which holds that “no private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first receives a written release executed by the subject of the biometric identifier or biometric information”.

The Court applied a two-step test of concreteness to “ascertain whether the plaintiffs suffered a concrete injury-in-fact due to the violation” [p. 11]. First, the panel considered “whether the statutory provisions at issue were established to protect [the plaintiffs’] concrete interests (as opposed to purely procedural rights)”; second, the Court examined “whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests” [p. 12].

To examine the first principle the Court recalled that “violations of the right to privacy have long been actionable at common law”, *Eichenberger* v. ESPN, Inc., 876 F.3d 979, 983 (9th Cir. 2017). Next, the Court affirmed that the right to privacy includes “the individual’s control of information concerning his or her person” [p. 16]. However, once Facebook creates a face template through its face recognition technology users lose control over their biometric information. Facebook can not only identify individuals in other photographs uploaded on the platform, but also determine their location at a given date. It follows then that the use of these biometric information without the users’ consent invades their private and concrete interests. In consequence, the Court concluded that the statutory provisions in BIPA were established to protect the individuals’ concrete interests in privacy, not merely procedural rights [p. 18]. This conclusion is supported by the Illinois Supreme Court precedent *Rosenbach*, 2019 IL 123186, which held that BIPA aims to protect individuals’ biometric privacy and therefore any violation of BIPA can aggrieve individuals because it “constitutes an invasion of the statutory rights of any person whose biometric identifier or biometric information is subject to the breach.” [p. 18].

Regarding the second principle, the Court found that since BIPA protects the rights of individuals not to be subject to the collection and use of their biometric data, then Facebook’s failure to comply with the statutory requirements of Sections 15 (a) and (b) necessarily violated the plaintiffs’ substantive privacy interests [p. 19]. This argument relies on the Illinois Supreme Court interpretation of the procedural protections of BIPA: “[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 [p. 19]. The Court also referred to *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017), which found that the mere “disclosure of an individual’s personally identifiable information and video viewing history” constituted a violation of the Video Privacy Protection Act sufficient to have Article III standing because it injured “the individual’s ‘substantive privacy interest in his or her video-viewing history’” [p. 19]. On the contrary, the Court rejected Facebook’s reliance on *Bassett v. ABM Parking Services, Inc.*, 883 F.3d at 780. In that case, the plaintiff failed to allege a concrete harm because the disclosure of his private financial information by a parking garage (on a receipt displaying his card’s full expiration date) did not impact his substantive rights under the Fair Credit Reporting Act, since only the plaintiff himself saw the expiration date [p. 20].

A second issue the Court considered was whether the district court abused its discretion by certifying a class action. Facebook argued that in virtue of the Illinois extraterritoriality doctrine “an Illinois plaintiff may not maintain a cause of action under a state statute for transactions that took place outside of Illinois” [p. 21]. Since Facebook’s data centers are located outside Illinois, “the necessary elements of any violation occurred extraterritorially” [p. 21]. Therefore, common questions do not predominate over questions affecting individual members and the district court erred in certifying the class. The Court ruled that BIPA applies to individuals who are in Illinois, “even if some relevant activities occur outside the state” [p. 22]. Consequently, “if the violation of BIPA occurred when the plaintiffs used Facebook in Illinois, then the relevant events occurred ‘primarily and substantially’ in Illinois” [p. 22]. Facebook’s second argument was that a class-wide statutory damages action was not superior to individual actions because it was not fairer and more efficient in adjudicating the controversy. Put simply, Facebook [argued](https://epic.org/amicus/bipa/patel-v-facebook/Patel-v-FB-9th-Cir-Redacted-Opening-Brief-Public.pdf) that a class cannot be certified if it creates the potential for a massive and disproportionate statutory award that would be inconsistent with legislative intent. The Court dismissed the argument and held that there were no grounds for denying class certification if the statutory language and the legislative history did not intend to place a cap on statutory damages [p. 23-24].

In conclusion, the Court considered there was sufficient ground to confer Article III standing for a class action complaint because “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” [p. 20]. In consequence, the Court rejected Facebook’s complaint for lack of Article III standing and Facebook’s appeal of the order granting class action certification.

**Decision Direction**

The decision expands freedom of expression for two reasons. First, because it establishes a [persuasive precedent](https://jolt.law.harvard.edu/digest/patel-v-facebook-facebook-settles-illinois-biometric-information-privacy-act-bipa-violation-suit) that makes it easier for individuals to protect their privacy rights. Under the Court’s broad interpretation of “injury in fact”, any failure to comply with BIPA’s procedural regulations constitutes a violation of an individual’s privacy rights and an intangible injury sufficient to establish liability. In practice, this means that plaintiffs do not need to allege a particular monetary, emotional, or reputational harm to have standing to sue for damages, other than the private entity’s breach of the statute. Second, because as in the [*Robins v. Spokeo* 867 F.3d 1108 (9th Cir. 2017)](https://harvardlawreview.org/2018/01/robins-v-spokeo-inc/), the decision “preserves the vitality of class action litigation as the best mechanism for protecting against online abuses”. All these reasons restrict the power of companies to operate unchecked and [help](https://digitalcommons.law.ggu.edu/cgi/viewcontent.cgi?article=2229&context=ggulrev) “enforce higher data privacy standards”.

**Global Perspective**

The Court has a national perspective and does not reference case law from other countries or regional courts, or international standards.

**Table of Authorities**

* U.S. Const. art. III, § 2, cl. 1.
* Biometric Information Privacy Act, 740 Ill. Comp. Stat. §14/1-14/99 (2008).
* *Rosenbach v. Six Flags Entm’t Corp*., IL 123186 (2019). Referenced by the Court to determine whether the breach of BIPA’s procedural provisions generates a concrete harm on individuals.
* *Lujan v. Defs. Of Wildlife*, 504 U.S. 555 (1992). Referenced by the Court on the constitutional minimum to have Article III standing in cases related to privacy rights.
* *Robins v. Spokeo* 867 F.3d 1108 (9th Cir. 2017). Referenced by the Court on the constitutional minimum to have Article III standing in cases related to privacy rights.
* *Bassett v. ABM Parking Services, Inc.*, 883 F.3d. 776 (9th Cir. 2018). Referenced by the Court on the constitutional minimum to have Article III standing in cases related to privacy rights.
* *Eichenberger v. ESPN, Inc.*, 876 F.3d 979 (9th Cir. 2017). Referenced by the Court on the constitutional minimum to have Article III standing in cases related to privacy rights, and on whether BIPA protects individuals’ concretes interests or procedural rights.