

## **Case Analysis Template**

### **Patel v. Facebook**

#### **Summary and Outcome**

The United States Court of Appeals for the Ninth Circuit held that facial-recognition technology used to create face templates without prior consent invades individuals' interests and privacy. In 2010, Facebook started using facial-recognition technology to develop its Tag Suggestions feature without the users' prior written consent and without a retention schedule of the biometric information. Three Facebook users in Illinois filed a complaint in 2015, alleging that Facebook's facial-recognition technology violated Illinois law. The Court affirmed the decision of the United States District Court for the Northern District of California, expressing that the right to privacy implies that individuals have control over their information. Facial-recognition technology allows Facebook to use detailed information of people without their consent. Thus, the Court concluded that Facebook's facial-recognition technology affected and invaded users' privacy and personal affairs.

#### **Facts**

The plaintiffs Adam Pezen, Carlo Licata, and Nimesh Patel were Facebook users since 2005, 2009, and 2008, respectively. In 2010, Facebook implemented a new feature named Tag Suggestions that use facial-recognition technology to identify individuals in photos uploaded by the user who enabled the Tag Suggestions function. To develop this technology, Facebook stores face templates in its data centers.

The plaintiffs, who live in Illinois, acting as class representatives, filed an operative complaint against Facebook in August 2015, alleging that Facebook's facial-recognition technology violated the Illinois Biometric Information Privacy Act (BIPA).

The plaintiffs claimed that Facebook violated Section 15(a) and 15(b) of the BIPA because it collected and used users' biometric information, specifically their face templates, without their prior written consent, to develop the Tag Suggestions feature. Also, the plaintiffs considered that Facebook violated the BIPA because it did not have a retention schedule for the destruction of biometric identifiers. Sections 15(a) and 15(b) of the Illinois Biometric Information Privacy Act provide obligations and requirements as "establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information"<sup>i</sup> and "to notify the individual in writing and secure a written release before obtaining a biometric identifier" [p. 9].

Facebook, the defendant, filed a motion to dismiss the complaint arguing that the plaintiff did not prove the existence of an injury-in-fact.

The district court's order certified the class and "denied Facebook's motion to dismiss" [p. 10]. The defendant filed a petition to appeal the district court's decision. The United States Court of Appeals for the Ninth Circuit considered it had jurisdiction to review the district court's ruling.

#### **Decision Overview**

Judge Ikuta delivered the judgment for the Court.

## Case Analysis Template

### Patel v. Facebook

The main issue brought before the Court was whether Facebook violated Sections 15(a) and 15(b) of the Biometric Information Privacy Act and users' right to privacy using the facial-recognition technology.

The plaintiffs alleged that Facebook violated sections 15(a) and 15(b) of the BIPA and the plaintiffs' privacy rights.

On the other hand, Facebook considered that the plaintiffs described procedural violations in the complaint and argued that the plaintiffs did not allege an injury-in-fact.

The BIPA provided obligations for private entities in possession of biometric information to protect individuals' privacy rights. The obligations of Sections 15(a) and 15(b) included the establishment of a retention schedule regarding the destruction of the biometric information and the need to obtain a written release "executed by the subject of the biometric identifier or biometric information".<sup>ii</sup>

The Court divided its analysis into two issues. The first issue raised by the Court was whether the Biometric Information Privacy Act protected plaintiffs' concrete interests "(as opposed to purely procedural rights)" [p. 12]. The second issue raised by the Court was whether the violations that the plaintiffs alleged harmed or presented "a material risk of harm to, such interests" [p. 12].

With reference to the case U.S., *Kyllo v. United States*, 9th Cir. 533 U.S. 27 (2001), the Court started its analysis, noting that technology developments imply more risks for the right to privacy, especially more intrusions into personal privacy.

The Court mentioned various judgments of the Supreme Court to demonstrate that the use of technology causes more violations and intrusions of the right to privacy. In fact, the Court concluded that in the case, the facial-recognition technology allows Facebook to obtain detailed information and invade users' personal affairs due to the creation of the face template. Within these personal affairs, the Court mentioned especially relevant information like the users' location or identification of the users' friends.

Therefore, the Court concluded 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" [p. 17].

Additionally, the Court referred to the Illinois General Assembly, which noted the importance of creating provisions to protect the right to privacy regarding individuals' biometric information. The Assembly stated the provisions' relevance based on the risks that biometric information use poses, including security and public welfare issues. Also, the Court established that the principal purpose of the BIPA was to protect individuals' biometric privacy, and it supported this statement in the U.S. case *Rosenbach v. Six Flags Entertainment Corp.*, IL 123186 (2019), in which the Illinois Supreme Court considered that privacy protection was the first function of the BIPA.

In the same case, the Illinois Supreme Court established that an individual could suffer harm due to the violation of BIPA when a private entity does not comply with its obligations according to Section 15 because that violation causes an invasion of the individuals' rights [p. 18].

Therefore, the Court established that BIPA provisions protect individuals' concrete interests and privacy.

## **Case Analysis Template**

### **Patel v. Facebook**

The second question raised by the Court was “whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests” [p. 18].

With reference to the US case of *Rosenbach v. Six Flags Entertainment Corp.*, IL 123186 (2019), the Court stated that BIPA provisions are essential to protect privacy rights in a digital world. According to the Court’s analysis, the BIPA protect the individuals’ right to privacy, which implies that no private entity may use or collect a person biometric information without its consent.

The described analysis allowed the Court to conclude that the plaintiffs alleged a concrete injury-in-fact because violations of Sections 15(a) and 15(b) of BIPA harm privacy interest or pose material risks of damage.

In conclusion, the United States Court of Appeals for the Ninth Circuit held that Facebook invaded the plaintiffs’ interests and privacy when it used the facial-recognition technology without their consent, violating Section 15(a) and 15(b) of the BIPA [P. 17].

#### **Decision Direction**

The decision expands expression because it protects the right to privacy, allowing plaintiffs to select the information they wish to share publicly and allowing them to control their information.

#### **Global Perspective**

##### **International, Regional, and National Laws or Cases**

U.S., *Rosenbach v. Six Flags Entertainment Corp.*, IL 123186 (2019)

U.S., *Kyllo v. United States*, 9th Cir. 533 U.S. 27 (2001)

U.S., *United States v. Jones*, U.S. 10-1259, (2011)

U.S. *Carpenter v. United States*, U.S. 16-402 (2018)

U.S. *Riley v. California*, 573 U.S. 373 (2014)

---

<sup>i</sup> U.S., IL Biometric Information Privacy Act Sec. 15(a)

<sup>ii</sup> U.S., IL Biometric Information Privacy Act Sec. 15(a)