Updates
February 04, 2020

New Biometrics Lawsuits Signal Potential Legal Risks in AI

In the last week, a new type of BIPA case has emerged that should be of interest to companies involved in using, improving, and developing facial recognition and other artificial intelligence (AI) using photos. Companies that deal with biometrics are likely aware of Illinois' Biometric Information Privacy Act (BIPA), which regulates the collection, storage, and use of biometric data, including, for example, fingerprints, voiceprints, and scans of "face geometry." BIPA permits plaintiffs to recover $1,000-$5,000 per violation, which can lead to staggeringly high damages exposure where large classes are involved. As a result, over 500 putative class action lawsuits have been filed in Illinois in the last five years against companies across the country.

Most BIPA cases target companies that collect or possess fingerprint data—for example, employers that require their employees to use fingerprints for timekeeping purposes. About a dozen cases target companies alleging that they use facial recognition technologies, such as companies that may use facial recognition to enhance services to customers, B2B companies that provide identity verification services, and brick-and-mortar stores that plaintiffs allege use facial recognition to track customers or for security purposes. A smaller handful of cases allege the collection of voiceprints in violation of BIPA.

New BIPA Lawsuits

Between January 22 and 24, 2020, three new cases were filed, alleging BIPA violations based on facial recognition data drawn from publicly available photos. These cases represent an additional area of legal risk for many companies and could lead to a new wave of BIPA cases against companies engaged in AI and facial recognition research.

In the first case, *Janecyk v. International Business Machines* Case No. 2020-CH-833 (Circuit Court of Cook County, Illinois), IBM was sued in connection with its use of publicly available images to create the "DiF" (Diversity in Faces) dataset, as recounted in this article. The plaintiff, Tim Janecyk, alleges that he is a photographer who uploaded photographs of people—including himself—in sensitive situations like political rallies to the photo sharing site Flickr. He alleges that Flickr's former parent company used these and other images to create a database of 99 million images for use as a reference library to train AI models. Using this database, IBM coded a subset of the photographs to describe the appearance of the people in the photographs. IBM then offered its collection to researchers as a tool to help reduce bias in facial recognition models. Janecyk alleges violations of multiple subsections of BIPA, and seeks $1,000 to $5,000 per violation on behalf of all Illinois citizens "who had their biometric identifiers, including scans of face geometry, collected, captured, received, or otherwise obtained by IBM from photographs in its Diversity in Faces Dataset."

A few days after this complaint was filed, a different law firm filed a second complaint against IBM based on the same alleged conduct by IBM. That case is *Vance v. IBM*, Case No. 20-cv-577 filed in the U.S. District Court for the Northern District of Illinois. The complaint alleges violations of multiple subsections of BIPA and asserts claims for unjust enrichment and injunctive relief.

In a third complaint, plaintiff David Mutnik sued AI startup Clearview AI, as well as its founder Hoan Ton-Thot and principal Richard Schwartz, based on its creation of a facial recognition database of millions of Americans from photographs scraped from the internet. Clearview allegedly sold that database to over 600 law enforcement

agencies, as recounted in this *New York Times* article, and the complaint alleges that Clearview's database is used by law enforcement agencies and other private entities to biometrically identify individuals. The plaintiff is an Illinois resident who believes biometric data based on his face is included in the database. Like Janecyk, Mutnik alleges that the people whose biometric information is included in the database had no knowledge of, and did not consent to, Clearview's alleged conduct. The complaint alleges violations of BIPA as well as a variety of other claims, including constitutional claims under the First, Fourth, and Fourteenth Amendments. It seeks relief on behalf of two classes, one nationwide class of all American citizens whose images are in Clearview's database for whom Clearview scanned the facial geometry from those images (the "Constitutional Rights Class") and another class of people residing in Illinois for violations of BIPA in connection with the scanning of the facial geometry and sale or disclosure of those images (the "Illinois Class").

Takeaways

This new line of BIPA attack likely increases the risk associated with using publicly available images for purposes of facial recognition research and building data sets for machine learning. To mitigate BIPA risk and other risk associated with using data to train and develop AI models, companies should first inventory the source of all data used to train and develop AI. Second, companies should document the intellectual property rights and privacy consents associated with each data set. Once this auditing is complete, a company can more clearly evaluate the risks associated with each data set, and it can consider mitigation strategies. The IBM and Clearview cases demonstrate that, even for publicly available data, a plaintiff may claim that processing personal information without consent violates the law.

Organizations involved with biometrics should seek experienced counsel for assistance in mitigating risk.

This update was republished in *The Journal of Robotics, Artificial Intelligence & Law (*September / October Edition).

Authors

Debra R. Bernard

Of Counsel
DBernard@perkinscoie.com 312.324.8559

Susan Fahringer

Partner
SFahringer@perkinscoie.com 206.359.8687

Nicola Menaldo

Partner
NMenaldo@perkinscoie.com 206.359.8000

Explore more in

Privacy & Security Technology Transactions & Privacy Law Artificial Intelligence & Machine Learning

Related insights

Update

Ninth Circuit Rejects Mass-Arbitration Rules, Backs California Class Actions

Update

CFPB Finalizes Proposed Open Banking Rule on Personal Financial Data Rights