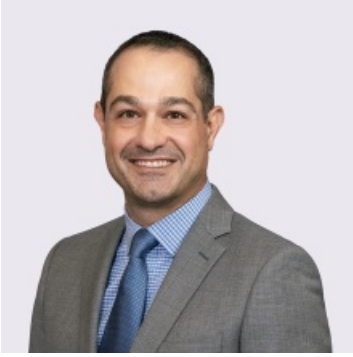
Special Report

Jump in Facial and Voice Recognition Raises Privacy, Cybersecurity, Civil Liberty Concerns

By Jason C. Gavejian, Joseph J. Lazzarotti & Jody Kahn Mason

February 3, 2022

Meet the Authors



Jason C. Gavejian
Office Managing Principal
908-795-5139
Jason.Gavejian@jacksonlewis.com

Joseph J. Lazzarotti
Principal
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com

Jody Kahn Mason
Principal

Facial recognition, voiceprint, and other biometric-related technology are booming, and they continue to infiltrate different facets of everyday life. The technology brings countless potential benefits, as well as significant data privacy and cybersecurity risks.

Whether it is facial recognition technology being used with COVID-19 screening tools and in law enforcement, continued use of fingerprint-based time management systems, or the use of various biometric identifiers such as voiceprint for physical security and access management, applications in the public and private sectors involving biometric identifiers and information continue to grow … so do concerns about the privacy and security of that information and civil liberties. Over the past few years, significant compliance and litigation risks have emerged that factor heavily into the deployment of biometric technologies, particularly facial recognition.

Biometrics Market

Research suggests that the biometrics market is expected to grow to approximately $44 billion in 2026 (from about $20 billion in 2020). This is easy to imagine, considering how ubiquitous biometric applications have become in everyday life. Biometrics are used for identity verification in a myriad of circumstances, such as unlocking smartphones, accessing theme parks, operating cash registers, clocking in and out for work, and travelling by plane. Concerns about security and identity theft, coupled with weak practices around passwords, have led some to ask whether biometrics will eventually replace passwords for identity verification. While that remains to be seen, there is little doubt the use of biometrics will continue to expand.

Increasing Concerns

A significant piece of that market, facial recognition technology, has become increasingly popular in employment and consumer areas (*e.g.,* employee access, passport check-in systems, and payments on smartphones), as well as with law enforcement. For approximately 20 years, law enforcement has used facial recognition technology to aid criminal investigation, but with mixed results, according to a New York Times report. Additionally, the COVID-19 pandemic has helped to drive broader use of this technology. The need to screen persons entering a facility for symptoms of the virus, including their temperature, led to increased use of thermal cameras, kiosks, and similar devices embedded with facial recognition capabilities. When federal and state unemployment benefit programs experienced massive fraud as they tried to distribute hundreds of billions in COVID-19 relief, many turned to facial recognition and similar technologies for help. By late-summer 2021, more than half the states in the United States have contracted with ID.me to provide ID-verification services, according to a CNN report.

Many have objected to the use of this technology in its current form, however. They

312-803-2535
Jody.Mason@jacksonlewis.com

Related Services

Biometrics
Privacy, Data and Cybersecurity

raise concerns over a lurch toward a more Orwellian society and related to due process, noting some of the technology's shortcomings in accuracy and consistency. Others have observed that the ability to compromise the technology can become a new path to committing fraud against individuals.

Additionally, the use of voice recognition technology has seen massive growth in the past year. A new report from Global Market Insights, Inc. estimates the global market valuation for voice recognition technology will reach approximately $7 billion by 2026. It said this is in main part due to the surge of AI and machine learning across a wide array of devices, including smartphones, healthcare apps, banking apps, and connected cars, among many others. While the ease and efficacy of voice recognition technology is clear, the privacy and security obligations associated with this technology, as with facial recognition, cannot be overlooked.

Illinois BIPA

With the increasingly broad and expanding use of facial recognition and other biometrics has come more regulation and the related compliance and litigation risks.

Perhaps one of the most well-known laws regulating biometric information is the Illinois Biometric Information Privacy Act (BIPA). Enacted in 2008, the BIPA was one of the first state laws to address a business's collection of biometric data. The BIPA protects biometric identifiers (a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry) and biometric information (any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual). The law established a comprehensive set of rules for companies collecting biometric identifiers and information from state residents, including the following key features:

- Informed consent in connection with collection
- Disclosure limitation
- Reasonable safeguard and retention guidelines
- Prohibition on profiting from biometric data
- A private right of action for individuals harmed by violations of the BIPA

The BIPA largely went unnoticed until 2015, when a series of five similar class action lawsuits were brought against businesses. The lawsuits alleged unlawful collection and use of the biometric data of Illinois residents. Since the BIPA was enacted, more than 750 putative class actions lawsuits have been filed. The onslaught is primarily due to the BIPA's private right of action provision. That provision provides statutory damages up to $1,000 for each negligent violation, and up to $5,000 for each intentional or reckless violation. Adding fuel to the fire, the Illinois Supreme Court ruled that an individual is aggrieved under the BIPA and has standing to sue for technical violations, such as a failure to provide the law's required notice. *Rosenbach v. Six Flags Entertainment Corp.,* No. 123186 (Ill. Jan. 25, 2019). While most of these cases involved collection of fingerprints for time management systems, several involved facial recognition, including one that reportedly settled for $650 million. In 2021, a new wave of BIPA litigation arose with the increased use of voice recognition technology by businesses. While general voice data is not covered by the BIPA, voiceprints have a personal identifying quality, thus potentially making them subject to the BIPA. For example, a large fast-food chain is facing BIPA litigation over alleged use of AI voice

recognition technology at their drive-throughs. Claims in both state and federal courts allege failures to implement BIPA-compliant data retention policies, informed consent requirements, and prohibitions on profiting and disclosure.

Many have argued that the BIPA went too far, opening the floodgates to litigation for plaintiffs who, in many cases, suffered little to no harm. Indeed, efforts have been made to moderate the BIPA's impact. However, massive data breaches and surges in identity theft and fraud have supported calls for stronger measures to protect sensitive personal information, including with regard to the use of facial recognition. At the same time, mismatches and allegations of bias in the application of facial recognition have led to calls for changes.

Fraud

In the last year, there has been an uptick in hackers trying to "trick" facial recognition technology in many settings, such as fraudulently claiming unemployment benefits from state workforce agencies. The majority of states are using facial recognition technology to verify persons eligible for government benefits to prevent fraud. The firm ID.me. Inc., which provides the facial recognition technology to help verify individual eligibility for unemployment benefits, has seen over 80,000 attempts to fool government identification facial recognition systems between June 2020 and January 2021. Hackers of facial recognition systems use a myriad of techniques including deepfakes (AI-generated images), special masks, or even holding up images or videos of the individual the hacker is looking to impersonate.

Fraud is not the only concern with facial recognition technology. Despite its appeal for employers and organizations, there are concerns over the technology's accuracy, as well as significant legal implications to consider. Importantly, there are growing concerns regarding accuracy and biases of the technology. A report by the National Institute of Standards and Technology said a study of 189 facial recognition algorithms considered the "majority of the industry" found that most of the algorithms exhibit bias, falsely identifying Asian and Black faces 10-to-beyond-100 times more than White faces. Moreover, false positives are significantly more common for women than men and higher for the elderly and children than middle-aged adults.

Regulations

A result has been increasing regulation of the use of biometrics, including facial recognition. Examples include:

- *Facial Recognition Bans.* Several U.S. localities have banned the use of facial recognition for law enforcement, other government agencies, or private and commercial use.
    - *Law enforcement bans.* Over the past few years, several states, cities, and localities have banned the use of facial recognition by law enforcement. These include Vermont, Virginia, San Francisco, Boston, New Orleans, and Minneapolis.
    - *Portland.* In September 2020, the City of Portland, Oregon, became the first city in the United States to ban the use of "facial recognition technologies" in the private sector. Proponents of the measure cited a lack of standards for the technology and wide ranges in accuracy and error rates that differ by

race and gender, among other criticisms.

The term "facial recognition technologies" is broadly defined to include automated or semi-automated processes using face recognition that assist in identifying, verifying, detecting, or characterizing facial features of an individual or capturing information about an individual based on an individual's face. The ordinance carves out limited exceptions, including the use of facial recognition technologies to comply with law, to verify users of personal and employer-provided devices, and for social medial application. Failure to comply can be painful. Like the BIPA, the provides persons injured by a material violation a cause of action for damages or $1,000 per day for each day of violation, whichever is greater.

- *Baltimore.* The City of Baltimore, for example, has banned the use of facial recognition technologies by city residents, businesses, and most of the city's government (excluding the police department) until December 2022. Council Bill 21-0001 prohibits persons from "obtaining, retaining, accessing, or using certain face surveillance technology or any information obtained from certain face surveillance technology." Any person who violates the ordinance is guilty of a misdemeanor and, on conviction, is subject to a fine of not more than $1,000, imprisonment for not more than 12 months, or both fine and imprisonment.

- *Biometrics, Generally.* Beyond the BIPA, state and local governments have enacted laws to regulate the collection, use, and disclosure of biometric information. Here are a few examples:

  - *Texas, Washington, and New York.* Both Texas and Washington have enacted comprehensive biometric laws similar to the BIPA, but without the same kind of private-right-of-action provision. New York, on the other hand, is considering a BIPA-like privacy bill that mirrors the BIPA enforcement scheme.

  - *The California Consumer Privacy Act (CCPA).* Modeled to some degree after the EU's General Data Protection Regulation (GDPR), the CCPA seeks to provide individuals who are residents of California ("consumers") greater control over their personal information. Cal. Civ. Code § 1798.100 *et seq.* Personal information is defined broadly and is broken into several categories, one being biometric information. In addition to new rights relating to their personal information (such as the right to opt out of the sale of their personal information), consumers have a private right of action relating to data breaches. If a CCPA-covered business experiences a data breach involving personal information, such as biometric information, the CCPA authorized a private cause of action against the business if a failure to implement reasonable security safeguards caused the breach. For this purpose, the CCPA points to personal information as "defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5." That section defined biometric information as "Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a

fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes." Cal. Civ. Code § 1798.150. If successful, a plaintiff can seek to recover statutory damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater, and injunctive or declaratory relief and any other relief the court deems proper. This means that, like under the BIPA, plaintiffs generally do not have to show actual harm to recover.

- *New York City.* The Big Apple amended Title 22 of its Administrative Code to create BIPA-like requirements for the retail, restaurant, and entertainment businesses concerning collection of biometric information from customers. Under the law, customers have a private right of action to remedy violations, subject to a 30-day notice and cure period, with damages ranging from $500 to $5,000 per violation, along with attorneys' fees.

In addition, New York City passed the Tenant Privacy Act, which, among other things, requires owners of "smart access" buildings (*i.e.,* those that use key fobs, mobile apps, biometric identifiers, or other digital technologies to grant access to their buildings) to provide privacy policies to their tenants prior to collecting certain types of data from them. It also strictly limits (a) the categories and scope of data that the building owner collects from tenants, (b) how it uses that data (including a prohibition on data sales), and (c) how long it retains the data. The law creates a private right of action for tenants whose data is unlawfully sold. Those tenants may seek compensatory damages or statutory damages ranging from $200 to $1,000 per tenant and attorneys' fees.

- *Other states.* Additionally, states are increasingly amending their breach notification laws to add biometric information to the categories of personal information that require notification, including 2020 amendments in California, Vermont, and Washington, D.C. Moreover, there are a myriad of data destruction, reasonable safeguards, and vendor requirements to consider, depending on the state, when collecting biometric data.

Organizations that collect, use, and store biometric data increasingly face compliance obligations as the law attempts to keep pace with technology, cybersecurity crimes, and public awareness of data privacy and security. It is critical that they maintain a robust privacy and data protection program to ensure compliance and minimize business and litigation risks.

Please contact a Jackson Lewis attorney if you have any questions.