Debevoise & Plimpton

Debevoise Update D&P

Face Forward: Strategies for Complying with Facial Recognition Laws
Part 1: The Current Patchwork

October 20, 2021

Two huge crosscurrents are sweeping the world of facial recognition—and moving head-on into each other. Companies are eagerly adopting facial recognition tools to better serve their customers, reduce their fraud risks, and manage their workforces. Meanwhile, legislatures and privacy advocates are pushing back hard. They challenge facial recognition as inherently overreaching, invasive of privacy, and prone to error and bias. Legal restrictions of different kinds have been enacted around the country, seemingly with more to come.

How will the tension sort itself out between new use cases, on the one hand, and the push for legal restrictions, on the other—and when? And what's a company to do right now, with facial recognition opportunities presenting themselves today while the law remains a moving target?

This two-part series aims to help. In this Part 1, we lay out the current laws governing facial recognition in the United States. In Part 2, we assess where the law is headed and offer some practical risk-reduction strategies.

I. THE PATCHWORK OF CURRENT FACIAL RECOGNITION PRIVACY LAWS

A. What Is Facial Recognition?

Facial recognition technology essentially attempts to turn your face into a fingerprint. The technology starts with a digital facial image. The image is then turned into a biometric template that can be compared to another template in search of a match. That match can be either to a specific person or to a category, such as age or gender. For purposes of these blog posts, we focus mainly on the former use case—matching a face to a specific person for identification purposes—rather than other use cases such as emotional evaluation and lie detection. Facial recognition scanning can be done on a small scale (your phone comparing your face to a local reference image in order to unlock), or on a large scale (capturing the face of every passerby in a crowd in search of, say, a security threat). Whether the scans are individual or mass, the data retention brief or long-term, the resulting templates are biometric identifiers. These biometric identifiers are the subject of an increasing number of privacy laws.

For any reader looking for a more detailed primer on how facial recognition works, we recommend this from the Center for Strategic & International Studies or this from Wirecutter.

B. How Is Facial Recognition Being Used?

A few real-world examples of how facial recognition is used will help set the stage for our legal discussion.

- **User Authentication**: People use facial recognition every day in lieu of passwords, thumbprints, or ID cards to gain access to their iPhones or to enter their offices.

- **User Security Authorization**: In addition to using facial recognition to permit entry, businesses also use facial recognition to identify criminals or other individuals that they prefer to *exclude*. For example, casinos may try to identify known cheaters or stores may try to identify shoplifters and criminals.

- **Marketing**: In the retail context, facial recognition or "facial detection" technologies can scan shoppers for features such as age, gender, and mood—then deliver tailored advertisements in real time.

- **General Surveillance**: As the pandemic has shifted many to remote or hybrid work, employers have stepped up the use of facial recognition to keep track of employees' productivity. Facial recognition is also being used to proctor bar exams and other kinds of tests.

- **Law Enforcement**: Law enforcement's use of facial recognition—for example, to pick out named individuals from photos, videos or live crowds—is controversial. Particularly scrutinized is the use of "real-time" facial recognition to scan crowds in public places, such as marches and protests. Advocacy groups have gathered their forces at https://www.banfacialrecognition.com/.

- **Helping Those with Low or No Vision**: The AARP touts a small wireless camera that attaches to eyeglasses, scanning nearby faces to help the wearer identify "your spouse, grandkids or coworkers." Facial recognition is also being used to improve social media access for the blind.

- **Digital Doorbells**: If any more evidence is needed that facial recognition technology has hit the mainstream, consider CNET's review of the best facial recognition security cameras of 2021. These products are able to identify familiar faces, alert homeowners of unfamiliar or unwelcome faces, and provide general surveillance functions.

C. What Kind of Data Do Facial Recognition Laws Cover?

There is no single, comprehensive statutory approach in the United States for facial recognition. Rather, the law is a patchwork of state and local ordinances.

In general, facial recognition laws are a subset of biometric privacy law. Currently, there are three U.S. states with laws specific to biometric privacy—Illinois, Texas, and Washington. All three make reference explicitly or implicitly to facial data.

These laws take two general approaches to defining what data is covered. The first is to regulate certain *types* of data, while the other is to regulate data that has the *capability* to identify an individual:

- Illinois and Texas take the first approach and use the term "biometric identifier" to refer to specified forms of recorded data, *i.e.*, "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." A "scan of . . . face geometry" refers to the process of measuring multiple specific aspects of the face, such as distance between the eyes and from chin to forehead. The resulting digital dataset is intended to make the face recognizable later when matched against a reference image.

- Washington, by contrast, uses catchall language focused on the ability of an entity to use "unique biological patterns or characteristics" to "identify a specific individual." The word "face" is not found in the statute, but facial recognition data is clearly covered.

Some state legislatures take an approach similar to Washington's in their general data privacy laws. These laws do not target facial recognition in particular but regulate the use of biometric information (which includes many forms of facial data) among the many types of personal data that they cover. For example, the recently enacted California Privacy Rights Act (the "CPRA"), discussed below, defines biometric information as a covered form of data. The CPRA goes a step further and includes biometrics under the heading of "sensitive personal information," a category that conveys additional consumer rights.

Jurisdictions vary on whether photographs are covered as a form of biometric data. Illinois' Biometric Information Privacy Act ("BIPA") excludes both "digital photographs" and "information derived from" photographs from the definition of "biometric information." California's data breach notification law, on the other hand, specifically *includes* digital photographs "used or stored for facial recognition purposes" in its definition of "unique biometric data" that—if breached—would trigger notification requirements.

D. What Do Facial Recognition Laws Currently Require?

1. Jurisdictions Expressly Banning Facial Recognition Technologies

The most restrictive regulations on facial recognition in the United States have come from city councils. Across the country, municipalities have passed laws banning the use of facial recognition technologies by state and local agencies, especially police departments. Legislative bodies have noted evidence that facial recognition technologies can have a disproportionate and adverse impact on marginalized communities, including due to bias in their ability to correctly identify women and people of color.

As of today, such bans have been passed in cities in California (Alameda, Berkeley, Oakland, and San Francisco); Massachusetts (Boston, Brookline, Cambridge, Northampton, Somerville, and Springfield); Jackson, Mississippi; King County, Washington; Portland, Maine; Portland, Oregon; Madison, Wisconsin; Minneapolis, Minnesota; Hamden, Connecticut; and New Orleans, Louisiana. Other cities, such as Davis, California; Pittsburgh, Pennsylvania; and Nashville, Tennessee have also passed ordinances regulating the use of surveillance technology using facial recognition.

At the state level, California has banned law enforcement from installing, activating, or using biometric surveillance with body cameras until 2023. Vermont and Virginia have banned law enforcement from using facial recognition technology pending further legislative action. While not an outright ban, Massachusetts has passed a statewide restriction on facial recognition use by law enforcement that requires, among other things, the use of a warrant to use_facial recognition technology in criminal investigations. New York State has banned the use of facial recognition in public and nonpublic schools, including charter schools, pending a report by the commissioner of education to be prepared in consultation with stakeholders.

Most facial recognition bans do not cover private companies. Maryland, at the state level, and two cities—Portland, Oregon and Baltimore, Maryland—are exceptions in that they do limit what the private sector can do:

- **Maryland**: Maryland has banned employers from using "facial recognition services"—defined as "technology that analyzes facial features and is used for recognition or persistent tracking of individuals in still or video images" during applicant interviews without notice and written consent.

- **Portland**: Portland's ordinance bans the use of facial recognition technologies by "private entit[ies]" within the city's limits. It defines "face recognition" as "the automated searching for a reference image in an image repository," along with the corresponding verification of that search's success. There is a private right of action: violators are subject either to actual damages or damages of $1,000 per day per violation, whichever is greater. Portland has three exceptions to its ban on private entities' use of facial recognition, which allow use: (1) where needed to comply with local, state, or federal laws; (2) where needed to verify individuals on personal or employer-issued communication devices, such as Apple's FaceID for iPhone; and (3) in social media applications, such as Snapchat or Instagram.

- **Baltimore**: Baltimore's ordinance, which applies to both public and private sector uses of the technology, prohibits individuals and businesses from obtaining, retaining, accessing, or using any face surveillance system or any information obtained from a face surveillance system in Baltimore City. Violating the ordinance is a misdemeanor. Those convicted may be subject to a fine of up to $1,000 or imprisonment for up to 12 months or both.

The Baltimore ban does have a carve-out permitting any "biometric security system designed specifically to protect against unauthorized access to a particular location or an electronic device." The ban also exempts the Maryland Image Repository System, which allows law enforcement to compare images against a database drawn from motor vehicle records and mugshots.

Baltimore's ordinance sunsets on December 31, 2022, unless the City Council finds that the prohibitions remain in the public interest, in which case the ordinance may be extended for five more years.

2. New York City: Regulating Facial Recognition Technology.

New York's City Council has passed two ordinances regulating, but not banning, uses of biometric identifiers including facial recognition technology.

New York City's new "biometric identifier information" law, passed in July 2021 and effective in January 2022, includes a "scan of face [] geometry" among the types of covered data. The law contains two main requirements.

- The first requirement is limited to "commercial establishments," defined as restaurants, retail stores, sports arenas, museums, concert venues, and theaters. These public-venue types of businesses must publicly display notices that they are collecting biometric information.

- The second requirement is an outright ban on "exchang[ing] anything of value or otherwise profit[ing] from the transaction of biometric identifier information." This language in the ordinance does not include the express limitation to "commercial establishments." But legislative history and the totality of the ordinance suggest that the profit limitation—like the disclosure requirements—applies only to the specified types of public venues.

New York City's new ordinance provides a private right of action. People can sue if the source of the violation is not cured within 30 days after the individual has provided notice to the business. In response to a complaint, a business must provide an "express written statement" that the violation has been cured in order to avoid a suit under this provision. Failure to cure and notify could be costly: the law authorizes individuals to collect damages per violation plus attorneys' fees.

Notably, the law does not apply to the use of biometric identifiers "by government agencies, employees or agents." Financial institutions also are expressly excused from the disclosure requirement.

New York City also recently passed the Tenant Data Privacy Act (the "TDPA"). The TDPA imposes myriad requirements on residential landlords using smart access systems that collect biometric information including "scan[s] of face geometry."

The TDPA requires residential landlords to provide written disclosures concerning their use of smart access systems, to obtain written consent from tenants to collect biometric information, and to implement stringent security measures to protect such information. The TDPA prohibits landlords from selling, leasing, or disclosing biometric information and from using a system to capture the reference data of a minor, or sharing such data, without written authorization of a parent or guardian, among other things.

The TDPA provides for a private right of action for violation of the prohibition to sell, lease, or disclose data. Compensatory damages or damages between $200 and $1,000 are authorized for each unlawful sale, as are reasonable attorneys' fees and court costs.

3. State Laws Permitting but Regulating Collection and Use of Biometric Identifiers, including Facial Data.

As noted, currently, only Illinois, Washington, and Texas have laws at the state level that aim to expressly and comprehensively address biometric privacy. The notice and consent provisions of these laws may pose hurdles for facial recognition because of the likelihood that the technology will collect biometric identifiers from those passing by. Depending on the context, it may or may not be possible to give effective notice to, or get effective consent from, all passersby.

a) Illinois

The first biometric privacy law in the United States was BIPA, which became effective in 2008. The Illinois legislature announced that it aimed to protect consumers whose fingerprints and facial scans were being used in "new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias."

Notable requirements of BIPA include:

(1) **<u>Retention/Destruction Schedule.</u>** Companies must develop and make publicly available a written policy on retention and destruction of biometric identifiers. The statutory retention period is either (i) three years following an individual's last interaction with the company or (ii) when the purpose of the identifier has been fulfilled, whichever comes first.

(2) **<u>Notice and Consent.</u>** BIPA imposes a notice-and-consent regime on companies that collect, capture, purchase, receive through trade, or otherwise obtain someone's biometric identifiers. This regime requires that the subject be informed in writing about the collection of biometric identifiers—including the purpose for collecting them and the length of time that they will be stored. The individual must then consent in writing.

The consent requirement applies to companies that "collect, capture, purchase, receive through trade, or otherwise obtain" biometric identifiers. Therefore, transferring biometric identifiers to third parties or vendors not named in the initial notice and consent interaction may expose companies to liability under BIPA. Plaintiffs are currently testing this possibility by bringing suits against third-party suppliers of systems that utilize biometric identifiers, such as biometric timeclocks used for signing in and out of work. *See, e.g., Figueroa v. Kronos Inc.*, 454 F. Supp. 3d 772 (N.D. Ill. 2020) (denying motions to dismiss and to strike class allegations against manufacturer of biometric timeclocks where plaintiff-employees did not receive notice or give consent to manufacturer).

Plaintiffs are also testing whether this requirement applies to businesses that collect the biometric identifiers of passersby, such as when a casino or store uses surveillance cameras equipped with facial recognition to scan individuals for purposes of identifying criminals or individuals known to cause disturbances. *See, e.g., Pruitt v. Par-A-Dice Hotel Casino, No. 1:20-CV-1084-JES-JEH, 2020 WL 5118035 (C.D. Ill. Aug. 31, 2020)* (denying a motion to dismiss where a casino was using surveillance technology to conduct facial geometry scans of individuals without their consent; holding that plaintiffs had sufficiently pled facts to assert a BIPA violation).

(3) **Limitations on Monetization and Profit.** BIPA features a blanket prohibition on selling, leasing, trading, or otherwise profiting from a person's biometric identifiers. While the law does not clarify the meaning of this prohibition, at least one court has construed "otherwise profiting" as falling in the same vein as "trading." *See Vance v. Amazon.com Inc.*, No. C20-1084JLR, 2021 WL 1401633, at *2 (W.D. Wash. Apr. 14, 2021) (interpreting "otherwise profiting" as limited to types of trading, selling, or leasing and as not encompassing improvements to the company's operations). The court held that "otherwise profiting" could cover instances where products are sold that use algorithms that were trained on biometric data, and courts continue to shape the contours of the prohibition. *See id. Compare, Vance v. Microsoft Corp.*, No. C20-1082JLR, 2021 WL 1401634, at *5 (W.D. Wash. Apr. 14, 2021) (finding that "otherwise profiting" was not adequately pled where there were no allegations that there was a direct sale of biometric data or that biometric data was essentially being disseminated by marketing the product).

(4) **Limitations on Disclosure.** BIPA prevents companies from disclosing biometric identifiers to third parties, except under a few specific circumstances including consented-to disclosure and disclosure necessary to comply with the law.

(5) **Duty of Care.** BIPA also requires companies to "store, transmit, and protect" biometric identifiers using a "reasonable" degree of care "that is the same as or more protective than" the way the company stores other confidential and sensitive information.

Notably, BIPA provides for enforcement by private citizens, with losing defendants on the hook both for generous statutory damages and for attorneys' fees. The Illinois Supreme Court has ruled that a plaintiff does not need to show real-world harm to state a successful claim—that is, a violation of the statute is enough. *See Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, 129 N.E.3d 1197 (finding that individuals need not allege actual injury or adverse effect beyond the violation of his or her rights under the act to be entitled to seek liquidated damages and injunctive relief).

Unsurprisingly, BIPA has begun to generate significant class action litigation both in Illinois and elsewhere:

- The *Six Flags* case, involving use of fingerprint scans for admission to a theme park, resulted in a $36 million settlement.

- Another case in Illinois involved the application of BIPA's written consent requirement to an online photo service that employed facial recognition, which led to a $6.75 million settlement. *See, e.g., Miracle-Pond v. Shutterfly, Inc.*, No. 19 CV 04722, 2020 WL 2513099 (N.D. Ill. May 15, 2020).

- *In re Facebook Biometric Info. Priv. Litig.*, 185 F. Supp. 3d 1155 (N.D. Cal. 2016) shows how plaintiffs can try and take BIPA "on the road," sustaining venues outside of Illinois and generating large settlements. Plaintiffs alleged that Facebook violated BIPA with its use of facial recognition software to scan uploaded photos and provide "tag suggestions" on subsequently posted photos without consent. Facebook settled for $650 million after the district court rejected dispositive motions by the company.

- In *Santana v. Take-Two Interactive Software, Inc.*, 717 F. App'x 12 (2d Cir. 2017), the plaintiffs challenged a feature of the NBA 2K video game that allowed them to scan their own faces and create basketball-playing avatars. The district judge held that plaintiffs lacked standing because they had not shown a material risk that their data would be improperly accessed by third parties, and thus failed to show a "risk of real harm" that was sufficient to create an injury-in-fact). The Second Circuit agreed.

- In *ACLU v. Clearview AI, Inc.*, Case No. 20-CH-4353 (Ill. Cir. Ct. Aug. 27, 2021), the court denied a motion to dismiss and rejected the argument that BIPA is unconstitutional under the First Amendment, finding that BIPA furthers an important governmental interest in preventing the unauthorized disclosure of biometric information. The court noted that BIPA does not prohibit the use of all face prints, but does require businesses to meet its notice and consent obligations for any involved Illinois residents. The court also held, as courts before it have, that BIPA requirements do apply when businesses derive biometric information from photographs (such as from a facial geometry scan), even if those photographs are publicly available.

b) Washington

Washington's biometric privacy law is similar to BIPA, but has five features distinguishing it from the Illinois law:

- Washington expressly distinguishes between biometric identifiers captured directly from individuals and those created from photographs or videos. The latter are excluded from regulation.

- It only applies to biometric identifiers that have been "enrolled." As defined in the statute, "enrollment" occurs when a company captures the biometric identifier, converts it into a reference template, and stores it in a database.

- Washington provides a safe harbor for the use of biometric identifiers for certain security purposes. The use of biometrics to prevent shoplifting, fraud, theft, and to protect the security or integrity of software, accounts, and people is not subject to the statute's requirements.

- Washington's law does not require written consent.

- Washington's law is only enforceable by the state attorney general.

Unlike BIPA, the Washington law has not yet been tested in the courts, nor has the Washington attorney general announced any enforcement actions arising under it.

c) Texas

Texas's biometric privacy law also imposes similar requirements to BIPA but allows more avenues for compliance. For example, in Texas, businesses have to inform individuals prior to capturing their biometric identifiers and obtain their consent—apparently in any form—whereas BIPA specifies that individuals must provide *written* consent.

Like Washington's, Texas' statute can only be enforced by the attorney general—with civil penalties capped at $25,000 per violation—and there are no reported cases or announcements of enforcement actions by the Texas attorney general.

4. General Privacy Laws That Also Address Biometrics

California, Virginia, and Colorado currently lead the nation in enacting comprehensive consumer data privacy laws. These laws are not focused on biometrics like those in Illinois, Texas, and Washington. Rather, they bring biometric identifiers into scope by including them in their definitions of "personal information" (California Consumer Privacy Act (the "CCPA")) or "sensitive" personal information (Virginia and Colorado, and California via amendments to the CCPA contained in the California Consumer Privacy Rights Act (the "CPRA")).

Under the CCPA, which is the only one of these state privacy laws currently in effect, consumers have a wide array of rights related to all of their personal information, including biometric identifiers. These rights include: the right to know which biometric identifiers the company collects; the right to opt out of the sale, if any, of that collected data; and the right to have biometric identifiers deleted, with certain exemptions.

The CPRA, effective January 1, 2023, will go further, allowing consumers, with certain exceptions, to limit the use and disclosure of biometric identifiers. Consumers will be able to, for instance, instruct a business to limit the use of such information to what is necessary to perform the services or provide the goods reasonably expected by the average consumer or other purposes delineated in the CPRA.

Both Colorado's Privacy Act and Virginia's Consumer Data Protection Act (VCDPA), effective on July 23, 2023 and January 1, 2023, respectively, go beyond the CCPA and CPRA by requiring that companies refrain from processing biometric identifiers without consent, defined as a freely given, specific, informed, and unambiguous agreement.

The consent requirement would raise the issue of the passerby problem for facial recognition technology that picks up on individuals for whom companies cannot meet notice-and-consent requirements. But like Washington, both Colorado and Virginia provide safe harbors for companies to "prevent, detect, protect against, or respond to security incidents."

5. State Data-Breach Notification Statutes Treating Biometric Identifiers as Notification Triggers.

All 50 U.S. states (and some U.S. territories) have laws requiring notification of data breaches in certain circumstances. Typical "trigger" elements, requiring notification for unauthorized acquisition of data, are traditional personal identifiers like passport and Social Security numbers.

In recent years, a number of states and Washington D.C. have added biometric identifiers as notification triggers. The states with such statutes include Arizona, Arkansas, California, Colorado, Delaware, Illinois, Iowa, Kentucky, Louisiana, Maryland, Nebraska, New Mexico, New York, North Carolina, Oregon, South Dakota, Vermont, Washington, Wisconsin, and Wyoming.

6. States Requiring "Reasonable" Security for Biometric Data.

In a growing trend, about 25 U.S. states now have laws that, in one form or another, call for "reasonable" security measures to be applied to personal data. A number of states include biometric identifiers among the types of data requiring reasonable security. The states with such statutes include California, Colorado, Illinois, Maryland, Texas, Virginia, and Washington.

What is "reasonable" typically goes undefined in these laws. It is generally understood that what is reasonable is an evolving concept: As threat vectors and "market" security practices evolve over time, so too will what amounts to "reasonable" and therefore legally compliant data security. Some jurisdictions, like New York State, through its SHIELD Act, have begun to impose specific requirements as to what is "reasonable."

* * *

This wraps up our review of where facial recognition law stands today. See Part 2 for our thoughts on where the law is headed, and strategies for coping with the legal uncertainties as the law keeps evolving.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Avi Gesser
agesser@debevoise.com

Johanna N. Skrzypczyk
jnskrzypczyk@debevoise.com

Anna R. Gressel
argressel@debevoise.com

Andres S. Gutierrez
asgutierrez@debevoise.com