Face Forward Part 2: Proposed Legislation and Strategies for Compliant Use of Facial Recognition

October 27, 2021

This is Part 2 in a two-part series of articles about facial recognition laws in the United States. In Part 1, we discussed how current legislation addresses facial recognition. In this part, we assess where the laws seem to be heading and offer some practical risk reduction strategies.

I. PROPOSED U.S. FEDERAL AND STATE LEGISLATION

There is currently no federal law that specifically regulates biometric privacy. Among other proposed federal legislation, the National Biometric Information Privacy Act of 2020 died in Congress last year. It would have borrowed heavily from Illinois's Biometric Information Privacy Act ("BIPA"), including the controversial private right of action. Additionally, nothing in the bill would have preempted "any Federal, State or local law that [would] impose[] a more stringent limitation than the limitations described" in the bill's requirements section.

States have proposed numerous bills in recent years that would constrain the use of biometric identifiers by commercial entities within their jurisdictions. Among the strictest proposals are Massachusetts' Senate Bill 46 and House Bill 142—two versions of the "Massachusetts Information Privacy Act" are currently pending.

Both Massachusetts bills would require ***handwritten*** consent from each individual whose biometric identifier is collected. This would seem to eliminate not just the possibility of compliance-by-signage but also the possibility of online consent. Massachusetts would also completely ban "monetizing" —a term defined broadly— biometric identifiers as well as geolocation data.

Additionally, beyond the initial collection, consent would need to be re-obtained "two weeks before changing the nature of the processing of [biometric identifiers]."

The Massachusetts bills would impose three separate duties on covered entities: a duty of care, a duty of loyalty, and a duty of confidentiality. The duty of loyalty would

prohibit companies from using biometric identifiers in ways that benefit themselves to the detriment of the individual who provided the information. It would also forbid using the data in ways that are foreseeably injurious or "highly offensive to a reasonable individual."

Senate Bill 220, which is specific to biometric data, is another Massachusetts bill that would require handwritten notice and consent from consumers before collecting, capturing, purchasing, receiving through trade, or otherwise obtaining biometric identifiers or biometric information. Like BIPA, it would prohibit businesses' selling, leasing, trading, or otherwise profiting from biometric identifiers or biometric information. It would also prohibit disclosure of such data, with limited exceptions. The bill would provide for a private right of action that allows consumers to obtain damages of no less than $5,000 per violation, as well as attorneys' fees. It would also allow the attorney general to bring an action for violations or suspected violations with damages set to the greater of $5,000 per violation or actual damages suffered.

In their last session, New York lawmakers introduced but did not pass Assembly Bill 27, the Biometric Privacy Act ("BPA"). If enacted, New York's BPA would impose essentially the same requirements for businesses as BIPA, including: (1) a publicly promulgated retention schedule and guidelines for permanent destruction; (2) written notice and consent requirements; (3) prohibition of selling, leasing, trading, or otherwise profiting from a customer's biometric identifiers; (4) prohibition of the disclosure, redisclosure, or dissemination of such identifiers unless there is consent or another exception is met; and (5) use of a reasonable standard of care at least as protective as for other confidential and sensitive information.

Like BIPA, the New York BPA would provide a private right of action for individuals and would allow for recovery of up to $5,000 per violation and for other relief. Given its similarity to Illinois's BIPA, if the New York BPA is enacted, it would likely make New York home to a flurry of class-action litigation.

Unlike the Washington law, the proposed Massachusetts and New York bills contain no safe harbors for security uses. Accordingly, they would seem likely to prohibit the use of facial recognition technology in "passerby" circumstances where companies cannot meet notice and consent requirements because, for instance, individuals have their faces scanned by surveillance cameras with facial recognition technology as they pass by a store.

Our focus here is the United States, but we will briefly and uncomprehensively address Europe. Per our recent post, the European Commission's draft regulation on artificial intelligence (AI) proposes to ban not only all "real-time" remote biometric identification systems used by law enforcement in public places—including facial recognition—but

would also impose stringent requirements on both "real-time" and post hoc remote biometric identification systems (including those used by private entities).

Further, in a case that we have covered previously involving a supermarket using video surveillance with facial recognition capabilities, the Spanish data protection authority (the "AEDP") fined grocer Mercadona for violating numerous provisions of the EU's General Data Protection Regulation. Mercadona used "real-time" facial recognition technology to detect known bad actors trying to enter the store, but the AEDP was concerned that, among other things, the technology worked by scanning all who entered, including employees and children. The AEDP issued Mercadona a fine of 2.5 million euros.

II. CUTTING THROUGH THE PATCHWORK PROBLEM: PRACTICAL STRATEGIES FOR USING FACIAL RECOGNITION IN LEGALLY COMPLIANT WAYS

As we've discussed, the law of facial recognition is a jurisdiction-by-jurisdiction patchwork. It is obviously easier for multistate companies to do business under a unified legal fabric. No comprehensive and preemptive federal law seems likely to pass anytime soon. For now, then, companies doing business on a multistate basis have to deal with the patchwork of conflicting state and local laws.

One option is to tailor business practices state by state and city by city so that the practices comply with the particulars of each local law. This approach would involve first excluding Portland, Oregon altogether from a company's initiatives involving facial recognition, given that it is the only U.S. jurisdiction to flatly ban private use of facial recognition.

Everywhere else, a company would match its initiatives to what each U.S. jurisdiction requires. For example, written consent would be obtained from consumers in Illinois (because BIPA mandates it), but other forms of consent might be obtained in Texas (whose law only requires "consent" but not necessarily in written form). This approach can be burdensome, but it gives businesses maximum freedom in jurisdictions that have either no biometric privacy laws or less restrictive ones.

The tailored, state-by-state approach is exemplified by the home security company Nest, owned by Google. With "familiar face recognition" technology, Google states, Nest users "can use familiar face detection to teach your Nest camera how to recognize faces of people that you know and notify you when it sees people you don't know." In an apparent concession that this technology cannot be squared with BIPA's written consent requirements, Nest has reportedly disabled the use of facial recognition for some of its products in Illinois.

An alternative approach is to apply *everywhere* the most rigorous legal standards found *anywhere*. This "highest-common-denominator" approach would mean voluntarily accepting compliance burdens in some places that do not currently require them—*e.g.*, getting written consent from customers in Texas even though it is only a requirement in Illinois. This approach can be a hard sell for lawyers talking to their business-side clients, for whom being a compliance volunteer is rarely popular.

The advantage of the highest-common-denominator approach is operational simplicity. A company would need just one set of policies, procedures, and technologies everywhere it operates. Another advantage is that with the trend line pointing toward more and not less legal restrictions on facial recognition, fewer changes to the business will be needed as more new laws come online. It should be noted that this approach likely does not work for companies that collect facial data from passersby, since consent (per BIPA) is an element of the highest common denominator, and companies likely cannot meet notice and consent requirements for those individuals.

Companies also have an even more rigorous, "future-proofing" option: going above the current highest common denominator by matching their business practices to requirements that seem likely to be adopted by legislatures in the future. An example might be Massachusetts' proposed requirement of *handwritten* consent. This approach promises a reduced need to amend business practices, as it anticipates the likelihood that the law will grow stricter in more jurisdictions over time.

Companies contemplating adoption of some form of the highest-common-denominator approach should consider:

- Adhering to the broader definitions of biometric identifiers. Internal policies and procedures around biometric data privacy could speak to all forms of biometric identifiers, not just the limited universe of hand, face, and iris scans covered by the narrower laws.

- Providing robust notice, and obtaining *written* consent, when collecting biometric identifiers. A compliant-everywhere form of *notice* could require that companies inform individuals that their biometric identifiers will be collected, the purpose for which the identifiers will be used, and how long they will be stored (the maximum being three years after an individual's last interaction with the company, in accordance with BIPA). Contemplated uses and vendor relationships could be disclosed as well.

  A "compliant-everywhere" form of *consent* could also require a written release by the individual in order to meet BIPA requirements (handwritten, if the company wants to be particularly conservative by anticipating Massachusetts). Colorado explicitly

prohibits the use of "dark patterns"—coercive strategies that are designed to extract consent through annoyance, mistake, or confusion—during any consent process.

- Creating written retention and destruction policies and making them available to the public. These policies could match the schedule outlined in the Illinois BIPA: permanent destruction of the identifier after either three years following the individual's last interaction with the company or after its purpose is fulfilled, whichever comes first.

- Exercising a "reasonable" degree of care when handling and storing biometric identifiers. At least as much care could be given to biometric data security as to other sensitive or confidential information.

- Refraining from disclosing biometric identifiers to any third parties without first engaging in a notice and consent process. As with privacy policies generally, notices could typically mention at least three possible scenarios in which disclosure of biometric identifiers may be made to third parties: (1) when disclosure completes a financial transaction requested by the individual whose identifier was collected; (2) when disclosure is required by local, state, or federal law; and (3) when disclosure is made pursuant to a valid subpoena or other legally enforceable request.

- Refraining from selling, leasing, trading, or otherwise exchanging biometric identifiers for something of value. Given that this provision of BIPA is currently being tested in the courts, this is also an important area for lawyers to monitor going forward.

- In public settings, displaying notices that biometric data collection is occurring. A "compliant-everywhere" approach could require signage to deal with the CCPA's requirement for notice at the time of collection and New York City law's signage requirement (and any copycats that emerge), while written consent could also be required to deal with Illinois BIPA and its followers.

- Providing consumers with robust notice of their rights. Consumer rights could include the right to know/access the biometric identifiers collected from them, notice of their right to request deletion of personal information, the means to exercise those rights, and an explanation that the company will not discriminate against them for exercising such rights. Companies could also implement policies and procedures to ensure that they are able to respond to such requests in a timely manner. And companies could implement processes to confirm that all issues that consumers raise are addressed and that resolutions are documented, so as to comply with the cure provisions of New York City's facial recognition law.

- Preparing to defend class actions. On the assumption that private rights of action will only expand, companies could consider reviewing their insurance policies to see if biometric privacy cases are covered; consider lining up appropriate outside counsel; and give preliminary thought to what defenses would be available. For example, tight version control could be exercised over all forms of notice and consent, with copies stored in a fashion that will be readily accessible to litigation defense counsel.

Even if a company does not want to take the highest-common-denominator approach, it might productively consider the following steps to help promote compliance with both current and future laws:

- **Assess Operations**: Companies may want to engage in internal fact-finding (questionnaires, interviews) to assess whether they are collecting or processing biometric identifiers that would be in scope under any current law. It may also be prudent to establish policies and procedures for any adoption of new biometric technologies—educating the business and technical teams on the need to check with the legal and privacy functions before taking new steps in the collection or use of biometric data.

- **Develop a Plan**: Companies could also consider developing protocols, and training employees across business units, to address the legal protections that apply to biometric identifiers. Key questions that businesses could plan to answer include (where biometric laws are applicable):

  - *Notice and Consent*. Have individuals received notice that their biometric identifiers are being collected? Has the company obtained those individuals' consent? Is that notice public? Does the mode of consent meet particular state-law requirements, *e.g.*, does the relevant jurisdiction have a written consent requirement? Where are the records of consent maintained? How is consent handled for minors or others who lack legal capacity?

  - *Transmission of Data into and Out of the Company*. Are biometric identifiers being transferred to other parties, including for profit? Are they being used only to support the company's own operations? What about any transfers to vendors? What security measures protect this data, both within the company and once transferred to other entities?

  - *Retention and Destruction*: Does the company have a written retention and destruction policy regarding biometric data? Is that policy also publicly available? Is it enforced internally?

- *Consumer Complaints*: Does the company have a mechanism to escalate and address consumer complaints? The New York City ordinance, as well as the CCPA/CPRA, contemplates that consumers can put businesses on notice of potential violations and start the clock running for the businesses' cure period that would forestall monetary damages. Does that mechanism account for cure periods, subsequent notice to the complainant, and other statutory requirements?

- *Compliance*. Does the company have methods to check compliance with legal requirements and with internal policies and procedures? Which team internally (*e.g.*, privacy, compliance, internal audit) "owns" this responsibility?

- **Integrate Vendors into Assessments**: A common scenario is when Company A hires Vendor B to process biometric identifiers of A's employees or customers. The contract between A and B is worth reviewing to ensure that it clearly spells out what data B will collect, how B will use it (including whether any downstream uses not for A's benefit are permitted), and how compliance responsibilities and legal liabilities are assigned. Particularly noteworthy is assessing whether the relationship with the vendor was adequately disclosed during the notice and consent interaction and how the vendor relationship relates to the company's disclosure and re-disclosure obligations when it comes to biometric identifiers.

- **Assess Risks Posed by Artificial Intelligence Systems**: Many of the technologies that leverage biometric identifiers rely on AI or machine learning ("ML") technologies to process biometric identifiers in real time and on a large scale. AI technologies—including facial recognition and other biometric-based technologies—have been widely alleged to reflect biases based on race, gender, or disability, among other factors. To the extent that a company uses AI/ML systems to process biometric identifiers, it should be attentive to the potential reputational and regulatory risks posed by their use as well as the prospect of more stringent regulation in this space by state, federal, and foreign regulators.

The authors thank Cameron Sharp, a 2021 Debevoise summer associate, for his substantial assistance with this post.

* * *

Please do not hesitate to contact us with any questions.

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