EVERSHEDS SUTHERLAND

Implications of US laws on collection, storage, and use of biometric information

Frank Nolan, Eversheds Sutherland (US) LLP

July 2020

The past few years have seen dramatic innovations in biometric technology and an accompanying exponential growth in the size of the biometrics industry, in part due to the spread of Internet of Things (IoT), artificial intelligence (AI), and edge computing products into businesses and homes across the globe.

Whether it is through a simple fingerprint or facial recognition scan to unlock a phone, access a bank account, or gain entry to a secure work area, most people have provided their biometric information to a private entity. Further, an increasing number of companies have adopted some form of biometrics in their day-to-day operations, most often resulting in the collection of such data from their customers or employees. Nearly every industry has found uses for biometrics, including in transportation, manufacturing, automotive, healthcare, education, insurance, banking, payments, fashion, real estate, and entertainment.

As is often the case, however, the technology has outpaced the law.

To date, only three states have enacted stand-alone legislation specifically addressing commercial collection, storage, and use of biometric information. Among those, only one – Illinois – provides a private right of action. Several state legislatures have proposed similar laws in the past few years, and a growing number of states have incorporated biometrics into their data breach notification statutes. At the federal level, biometrics are addressed in a small number of industry-specific statutes, the Federal Trade Commission (FTC) has issued nonbinding guidance, and a handful of bills have been proposed in the US Congress. In short, the legal landscape for biometrics in the United States is unsettled and developing.

The primary focus of this paper is to explain that landscape as it applies to companies using biometrics in the United States.[1]

About the author

Frank Nolan is a Partner in the Litigation Group of Eversheds Sutherland, and sits in the Firm's New York City office. As part of his consumer class action defense practice, Frank counsels clients employing biometric technology and defends against litigation arising from biometric protection and other privacy and data security laws. He can be reached at franknolan@eversheds-sutherland.com or +1 212 389 5083.

Overview of biometrics

Biometrics typically work by identifying an individual or verifying that person's identity. In both cases, the subject's biometric information is collected and then compared with a template or templates already contained in a system.

Examples of biometric data that can be collected to identify or verify an individual include fingerprint, facial structure, voice pattern, gait pattern, ear canal structure, palm print, vein pattern, and iris or retina image. An increasing number of systems use multiple pieces of biometric data, for example, a multifactor authentication system employing a retina scan and a voice scan. A user's behavioral traits can also be utilized in conjunction with biometric data such as combining the user's fingerprint scan with the user's recognized pattern of typing on their phone for continuous or passive authentication of the user's identity. Verifying and identifying individuals using biometrics is typically done in one of two ways: 1:1 verification and 1:N identification.

1:1 verification

With 1:1 verification, a single biometric template ("1") is maintained in a system, such as a fingerprint template contained in a phone. When the phone's owner scans his or her fingerprint ("1") on the phone's screen, that biometric information is compared with the template in order to confirm the identity of the owner of the phone. If the scanned fingerprint matches the template, the identity is verified and the phone unlocks.[2] Among its advantages, verification through biometrics eliminates the user's need to remember or carry a password, increases speed of access to the device, and reduces the opportunity for a wrongdoer to hack into the device.

1:N identification

With 1:N identification, the collecting party possesses templates for a number of subjects, such as on a company timekeeping database.[3] When an employee clocks in by scanning his or her fingerprint ("1") into the timekeeping system, that biometric image is compared with the set of templates ("N") in order to identify the employee. If the scanned fingerprint matches a template in the system, the employee is identified and can clock in to begin a shift.

Biometrics are frequently hailed as a faster, more reliable, more convenient, and more secure alternative to passwords and other traditional forms of security. Biometric information is generally not stored in the form in which it is captured. Instead, it is typically "de-identified." The aim is to prevent reverse engineering or reproduction of the biometric identifier by a third party, limit unfettered access to that data by the storing party, and minimize fallout from a breach, although breaches of biometric data have been few and far between.[4] On an individual level, multilayered, behavioral, and passive biometrics are designed in part to drive down what risks do still exist with respect to a wrongdoer hijacking a person's biometric information.

The present and future of biometrics

Just a few months ago, most people were unfamiliar with body temperature scanning or contact tracing, and remote learning and working were far from commonplace. There is also an increased focus on the more traditional conundrum of understanding who is accessing or otherwise utilizing commercial and residential property, and where and when. Biometrics can be incorporated into new and existing technologies that can help address these issues. As a result, companies that did not previously collect biometrics may face practical and legal questions about how best to retain, protect, and destroy that data.

Biometrics are sure to evolve and change with the times in other ways. It would be natural in the current environment to expect consumer aversion to the use of fingerprint scanners or other forms of biometric collection that involve touching publicly used devices or surfaces. Fortunately, the industry is in many ways primed to adapt to a climate where social distancing and avoiding contact with surfaces are of paramount concern. There have already been advances in the use of ultraviolet rays to disinfect fingerprint and hand palm readers, and adapting facial recognition software to remain effective even while the subject wears a mask. Improvements in contactless scanning, iris recognition, and voice pattern detection will contribute to what many are expecting to be accelerated growth of the biometrics industry in the near future.

> The use of biometrics should only continue to grow as we adapt to a COVID-19 and post-COVID-19 world.

Real and perceived risks

Like anything else, the use of biometrics is not without its risks and drawbacks, be they real or perceived. A unique potential harm could arise if a person's unencrypted biometric information falls into the wrong hands. Unlike a Social Security number, facial structure and fingerprints cannot be changed with relative ease. The inability to alter biometric information thus ultimately creates a much longer, if not indefinite, tail on the risk of identity theft. Unique privacy considerations are also at play given the inherent value of biometric information that does not exist in other forms of personally identifiable information (PII).

Inherent bias in biometric systems has also been identified as a potential concern.[5] Such bias derives from the creators of the systems and can manifest itself, for example, in false positives (incorrectly identifying a person based on an image) and false

> The inability to alter biometric information ultimately creates a much longer, if not indefinite, tail on the risk of identity theft.

negatives (failing to verify a correct person using that person's image). The level of bias in facial recognition software is generally considered to be declining – that is, improving – with each system iteration.

Another concern with respect to the collection of biometric data relates to what has been colloquially referred to as "mission creep," where information is collected for one intended purpose and then maintained indefinitely or used for another, originally unforeseen, purpose. This can arise in any number of contexts. For example, a company may collect a facial scan of a potential consumer to design the proper fit for a pair of eyeglasses and later decide to use the facial scan for demographic-driven marketing efforts without the consent or even knowledge of the consumer. Or an employer could collect an employee's fingerprint scan for timekeeping purposes and later try to use the fingerprint to run a criminal background check.

Finally, simply maintaining biometric data after its intended use has expired leaves at risk both the individual and the company collecting the data. Guidelines and policies governing the storage, use, and destruction of biometric information can help mitigate these risks and prevent unwanted consequences while also allowing employees, consumers, and commercial entities to enjoy the benefits of biometrics.

> Your password is just a password, but your voice, your face, your fingerprint – those things *are* you.

The playing field: existing biometrics statutes

Only three states – Illinois, Texas, and Washington – have enacted statutes specifically addressing private entities' practices with respect to biometric information. Significantly, none of these laws prohibits the collection, use, or storage of biometric information. Instead, the statutes impose varying consent and notice requirements with which most companies must comply.

The most well-known and restrictive of these laws is the Illinois Biometric Information Privacy Act (BIPA), which we will address first and in the most depth.

a. Illinois

BIPA sat relatively dormant for several years following its enactment in 2008. Then, beginning in about 2015, plaintiffs' firms began filing putative class action complaints against some of the most well-recognized companies in America. That trickle of cases has swelled to a tidal wave. Over the past few years, hundreds of complaints have been filed against companies of all sizes and across a range of industries.

BIPA class actions arise from the use of numerous forms of biometric technology. In some complaints, the plaintiffs allege that they were aware of the collection of their biometric data, but they did not consent or were not given notice as required by the statute (e.g., employers collecting fingerprints through timekeeping software[6] or customers submitting facial scans to purchase eyeglasses without the requisite form of notice[7]). In others, the plaintiffs allege that they were not aware – nor could they have known – that their biometric data was being collected (e.g., data-scraping of internet photos without the knowledge of the subject[8] or the capture of children's images without consent[9]).

> Concerns regarding privacy, security, and bias have served as the impetus for much of the existing legislation governing biometrics.

The proliferation of BIPA class action lawsuits is no surprise. First, the use of biometrics is growing rapidly in the private sector. Second, BIPA's private right of action includes an exceptionally rich incentive: liquidated damages of $1,000 per negligent violation ($5,000 per intentional or reckless violation), plus recovery of fees and costs, including legal and expert expenses, and no cap on damages.[10] In the class action setting, where potential class members can number in the hundreds or even thousands, potential damages for BIPA cases can be astronomical. Further, whether insurance coverage is available for defendants facing BIPA claims is still largely unresolved.[11]

i. What is covered by BIPA?

BIPA encompasses what it defines as "biometric identifiers" and "biometric information." Biometric identifiers include "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[12] Biometric information, in turn, is defined as "any information" based on a biometric identifier that can be used to identify an individual. According to one court, "whatever a private entity does in manipulating a biometric identifier into a piece of information, the resulting information is still covered by [BIPA] if that information can be used to identify the person," even if the resulting information is a "mathematical representation or, even simpler, a unique number assigned to a person's biometric identifier."[13]

It is equally essential to understand what kind of information BIPA does not cover. For example, writing samples, demographic information, physical descriptions, and biological materials covered by the Genetic Information Privacy Act are expressly exempt from BIPA. Courts have already interpreted the bounds of some of these exemptions. For example, photographs are excluded from the definition of a biometric identifier under BIPA,[14] and the definition of biometric information explicitly states that it does not include information derived from items excluded under the definition of biometric identifiers.[15]

Nonetheless, a number of class action lawsuits have arisen from allegations that individuals' biometric identifiers were gathered from photographs uploaded to the defendants' websites.[16] Some courts have held that a scanned photograph can be subject to the requirements of BIPA in certain circumstances.[17] Another notable BIPA exemption addressed by the courts encompasses biometric data "captured from a patient in a health care setting" or "collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act" (HIPAA).[18]

ii. Who is subject to BIPA?

BIPA regulates private (nongovernmental) entities that collect, store, use, or profit from biometric data belonging to Illinois residents.[19] Some private entities, however, are exempt, including financial institutions or affiliates subject to the privacy notice provisions of the Gramm-Leach-Bliley Act of 1999 (GLBA).[20] Plaintiffs asserting BIPA violations have mostly been employees or consumers whose biometric data was collected in the course of their employment or use of a defendant's commercial services.

iii. What does BIPA require?

BIPA imposes five general requirements on nonexempt private entities that use biometric data in one form or another.[21]

Consent: collection, use, storage

The majority of BIPA lawsuits thus far have alleged violations of Section 15(b), which imposes written consent requirements on private entities that "collect, capture, purchase, receive through trade, or otherwise obtain" an individual's biometric data. The obtaining entity must explain why and for how long the biometric data is being collected, stored, or used, and the individual (or that person's legally authorized representative) must execute a written release.[22]

Consent: disclosure and dissemination

BIPA includes a separate consent requirement for private entities that intend to disclose an individual's biometric data. Entities responding to warrants or subpoenas are not bound by this requirement, and neither are entities using the biometric data to complete a financial transaction by the individual. The consent requirements can be satisfied in the employment context by obtaining a written release as a condition of employment.[23]

Defendants in BIPA actions have raised various defenses grounded in both the US Constitution and BIPA itself, with varying degrees of success.

Prohibition against profiting

BIPA explicitly prohibits private entities from selling, leasing, trading, or "otherwise profit[ing] from" an individual's biometric data.[24] This has not generally been the subject of BIPA class actions to date, thus raising a question as to how broadly courts may ultimately interpret the phrase "otherwise profit."

Retention policy

Companies subject to BIPA must also develop, publish, and abide by a retention schedule for biometric data they collect.[25] Biometric data must be destroyed by the earlier of the time at which the purpose of the initial collection has been satisfied or three years from the last interaction between the entity and the individual.

Reasonable standard of care

Finally, entities possessing biometric data governed by BIPA must "store, transmit, and protect" biometric data (1) using the reasonable standard of care in the entity's industry, and (2) in a manner consistent with how the entity handles other sensitive information.[26] This two-prong requirement underscores the need for companies to incorporate biometrics into their data compliance programs and to stay abreast of both security threats and breach prevention and response best practices.

iv. Injury-in-fact and Article III standing

Class action complaints brought under BIPA thus far have not alleged that the plaintiffs' biometric data was unlawfully accessed, or that the plaintiffs' identities were stolen or compromised. Instead, these complaints typically allege that the plaintiffs did not provide consent for the defendant to collect, use, or store their biometric data as required by the law. Not surprisingly, then, the first line of argument for many defendants in BIPA class actions in federal court has often been that the plaintiff has not suffered an injury sufficient to confer Article III standing under the US Constitution.[27]

As a statutory matter, BIPA gives anyone aggrieved by a privacy violation under the act the opportunity to bring a claim. What constitutes an "aggrieved" person is not further defined under BIPA. Most federal courts in Illinois have generally held, in reaching decisions on motions to dismiss, that even if a person is "aggrieved" for purposes of satisfying the statutory requirement under BIPA, that allegation alone is not sufficient to satisfy the Article III standing requirement.[28] But at least one federal court in Illinois held, sua sponte, that a defendant's alleged violation of a plaintiff's right to privacy was enough to satisfy Article III standing.[29]

Further chipping away at the standing defense is a decision out of the Northern District of California, which held that BIPA codifies an individual right of privacy in one's biometric information, the violation of which constitutes a concrete injury; this decision was affirmed by the US Court of Appeals for the Ninth Circuit in August 2019.[30] More recently, the US Court of Appeals for the Seventh Circuit weighed in on standing, this time in the context of removal from state court, finding that an alleged violation of BIPA's Section 15(b) amounted to an injury-in-fact.[31] While this decision was favorable for the defendant who wanted to remain in federal court, future plaintiffs faced with motions to dismiss their BIPA claims for lack of standing will surely cite it in support.

There is no such standing requirement in the Illinois Constitution, and in January 2019, the Illinois Supreme Court confirmed that plaintiffs need not allege an injury-in-fact to pursue BIPA claims in Illinois state courts.[32] Not surprisingly, the number of BIPA complaints filed in Illinois state courts increased throughout 2019 and into 2020.

v. Other constitutional and statutory defenses

Lack of personal jurisdiction

Among these is a defense of lack of personal jurisdiction over the defendant, such as when an out-of-state defendant conducts limited, or even no, business within the venue state.[33]

Although most BIPA lawsuits have been filed against employers that collect their employees' biometric data through fingerprint or facial recognition scans, a subset of BIPA class actions have recently been filed against the manufacturers and/or operators of biometric data timekeeping systems. In two such cases, the plaintiffs did not allege that the defendant companies had direct contact with employees; rather, the plaintiffs alleged that the defendants, without obtaining consent from or giving notice to the plaintiffs, provided the plaintiffs' employers with the technology to collect, store, and use their biometric data (or collected and stored the data by way of a third-party's relationship with the plaintiffs' employers).[34] The defendants in these cases challenged the courts' jurisdiction, leading to different outcomes and highlighting the nuances of a personal jurisdiction defense.[35]

Personal jurisdiction is highly dependent on the level, incidence, and frequency of the defendant's Illinois contacts and/or biometric data collection.[36] This is particularly true when the defendant does not have direct contact with the plaintiff but has indirectly obtained the plaintiff's biometric data, for example.[37]

Extraterritoriality, the Dormant Commerce Clause, and preemption

Defendants located outside of Illinois have similarly argued that BIPA cannot be applied extraterritorially. One court found that there are indeed "legitimate extraterritoriality concerns," and that, "as a matter of law," BIPA does not apply extraterritorially. That said, the defense has not been sufficient – at least yet – to warrant dismissal of a BIPA claim.[38] The threshold question in determining whether a case involves a potential extraterritorial application of BIPA is whether the circumstances giving rise to the case took place "primarily and substantially" within Illinois.[39] If yes, then an extraterritoriality defense may not be viable. If no, then extraterritoriality, or the application of BIPA outside of its prescribed bounds, could provide a basis for dismissal. This highly fact-intensive inquiry means that the strength of an extraterritoriality defense may not be fully known until the parties have engaged in some discovery, including, for example, to determine how the defendant's biometric software technology works.[40]

The Dormant Commerce Clause, which limits states' authority to pass legislation impacting interstate commerce,[41] presents a related potential constitutional defense to BIPA. As with most of the other potential constitutional challenges to BIPA,[42] the strength of this argument remains largely unknown and also likely requires a factual inquiry.[43]

Preemption of labor laws is another jurisdictional defense potentially available to employers facing BIPA class actions. Some defendants have successfully argued that BIPA claims brought by employees are preempted by federal law, precluding the claims in part or in whole.[44] The viability of a preemption argument is specific to each complaint and the respective federal or state labor laws at issue.[45]

Statute of limitations

BIPA has no defined statute of limitations, and it is not necessarily clear when BIPA claims begin to accrue. The possible statutes of limitations are one year,[46] two years,[47] or five years.[48] As to the related issue of accrual, at least one court has found that where the plaintiff plausibly alleged her former employer failed to delete her biometric information pursuant to BIPA's three-year maximum retention requirement, her claim did not accrue until three years after her employment ended.[49] These issues will likely be heavily litigated in the years to come, including because they could provide a basis for dismissal or impact potential class size, damages, and settlement value.

Class certification

There are very few class certification decisions under BIPA to date. The fact patterns in BIPA cases could very well present challenges for plaintiffs seeking to certify a class. Issues such as consent and notice in particular could raise a host of individualized questions, which could therefore preclude a finding of commonality or predominance.[50]

b. Texas

In 2009, Texas enacted its own biometric privacy statute governing the "capture and use of biometric identifiers."[51] The Texas statute covers "biometric identifiers," which is limited to retina or iris scans, fingerprints, voiceprints, or the record of hand or face geometry. Exempt from the statute are voiceprints collected by a financial institution.

Under this statute, prior to the collection of a biometric identifier for undefined "commercial purposes," the collecting party must obtain informed consent from the individual. Once a biometric identifier is collected, the collecting party may not sell, lease, or otherwise disclose the information except in limited circumstances, such as to complete a financial transaction at the request of the owner or if the information is needed to respond to a warrant. Similar to BIPA, the Texas statute imposes a standard of reasonable care on the party storing or transmitting biometric data that is equivalent to how that party would handle other confidential information. Further, the collecting party must destroy biometric data within a reasonable time, or within one year of the date when the purpose for the collection ends.[52]

The Texas statute includes a civil penalty of up to $25,000 per violation, but is enforceable only by the Texas Attorney General.

c. Washington

The stated purpose of Washington HB 1493, enacted in 2017, is to "require a business that collects and can attribute biometric data to a specific uniquely identified individual to disclose how it uses that biometric data, and provide notice to and obtain consent from an individual before enrolling or changing the use of that individual's biometric identifiers in a database."[53]

"Biometric identifiers" under this statute are data "generated by automatic measurements of an individual's biological characteristics," including voiceprint, fingerprint, and other "unique biological patterns," but not including data generated from photographs or videos. The law imposes certain notice and consent requirements where biometric identifiers are collected for a "commercial purpose," which is defined as "in furtherance of the sale, lease, or distribution of biometric data to third parties for the marketing of goods and services which are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier."

Under the Washington statute, the collecting party cannot "enroll a biometric identifier in a database for a commercial purpose" without obtaining consent, providing notice, and ensuring that the biometric identifier will not be used for a

commercial purpose in the future. The notice requirement is satisfied if it is made reasonably available to the affected individuals. Notice and consent are "context-dependent." Further, the collecting party may not sell, lease, or otherwise disclose a biometric identifier without the individual's consent, subject to some exceptions, which include completing a transaction at the request of the individual or complying with a court order. There is no set retention period, so long as the biometric identifiers are not maintained longer than reasonably necessary.

Washington's statute does not cover noncommercial uses of biometrics. For example, it expressly exempts from its requirements businesses' collection of data for "security or law enforcement," which is defined as "preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value." Washington's statute does not apply to financial institutions covered by the GLBA or to activities covered by HIPAA, and does not provide for a private right of action. The Washington Attorney General's office has the power to enforce the statute pursuant to Washington's Unfair Business Practices Consumer Protection Act.[54]

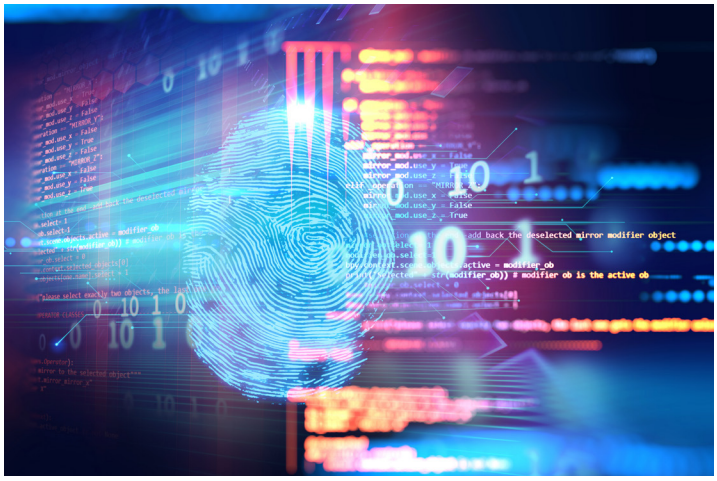
Biometric protections in other states

Several states have recently amended their breach notification and data protection laws to include biometric data among the protected types of information. In addition to the states discussed below, several other states incorporate biometric data in their breach laws.[55]

a. Arizona

Arizona's Data-Breach Notification Law governs entities that maintain unredacted or unencrypted information belonging to Arizona residents.[56] The statute defines "personal information" as a person's first or last name in combination with a "specified data element." Specified data element includes "[u]nique biometric data generated from a measurement or analysis of human body characteristics to authenticate an individual when the individual accesses an online account." Arizona imposes certain notice requirements following a data breach or "security incident." In addition to these notice requirements, the statute "encourages companies to adopt data-privacy and security policies with consumer-notification provisions in advance of any potential breach."[57]

The Arizona Attorney General may, pursuant to the Consumer Fraud Act, seek up to $500,000 in civil penalties plus restitution for knowing and willful violations of the statute.[58] As with many other statutes discussed here, entities covered by HIPAA or the GLBA are exempt.



b. Arkansas

In April 2019, Arkansas amended and revised that state's Personal Information Protection Act (PIPA) to expand the definition of personal information to include data "generated by automatic measurements of an individual's biological characteristics . . . ."[59] The law includes fingerprints, faceprints, retina and iris scans, hand geometry, voiceprint analysis, and DNA in its definition of biometric data. There is also a catchall definition of biometric data that leaves the door open for future technological developments: "[a]ny other unique biological characteristics of an individual if the characteristics are used by the owner or licensee to uniquely authenticate the individual's identity when the individual accesses a system or account."[60]

The Arkansas statute imposes notice requirements in the event of a breach,[61] and separately requires companies to implement security and destruction procedures and practices for covered information, including biometric data.[62] The Arkansas PIPA is enforceable by the Arkansas Attorney General.[63]

c. California

On January 1, 2020, the California Consumer Privacy Act (CCPA) went into effect.[64] The CCPA imposes stringent notice, consent, and retention obligations for consumer and employee "personal information" obtained by companies doing business in the state. The definition of personal information under the CCPA is broad and includes any information that "identifies, relates to, describes, and is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[65] The CCPA specifically includes biometric information as one of the categories of data that could fall under that definition of personal information.

The definition of biometric information is broader under the CCPA than under other laws, and includes behavioral information such as "keystroke patterns or rhythms." Significantly, however, personal information under the CCPA does not include information that has been "de-identified."[66] As discussed above, biometric information is often de-identified in some fashion. Whether a company's de-identification process meets the CCPA's statutory requirements appears to be a fact-specific inquiry. Further complicating matters is the current lack of guidance as to what constitutes "reasonable" measures to de-identify and the unknown extent to which outside hackers can re-identify data. In any event, although the CCPA's strictures could pose some level of risk to companies collecting biometric data, the security of biometrics may still pose an attractive alternative to the more traditional methods of identification and verification, such as through passwords and PII.

The CCPA is enforceable by the California Attorney General, but it does provide for a limited private right of action available to consumers in the event of a breach or disclosure of their personal information resulting from a company's failure to maintain reasonable security procedures.

It appears from the language of the CCPA that consumers may not tie violations of the CCPA to the California Unfair Competition Law in order to bring private litigation against companies, as is

possible under similar laws in other states.[67] That said, at least one plaintiff has attempted to do so in the biometrics context.[68] As a separate matter, a proposed California Privacy Rights Act (CPRA) is expected to be on the state ballot in November. The CPRA would expand consumers' privacy protections and rights, including as to biometrics, and would additionally create and empower a California Privacy Protection Agency to enforce the CPRA, separate and apart from the California Attorney General's office that currently enforces the CCPA.

d. Louisiana

Louisiana amended its Database Security Breach Notification Law effective August 2018.[69] The amendment to the law expands the definition of personal information to include biometric data, which is defined similarly to biometric data under the Arkansas PIPA. The Louisiana breach law requires that notice of a data event be provided to affected Louisiana residents and separately imposes data security and destruction requirements on covered entities.[70]

> It is only a matter of time before more states join Illinois, Texas, and Washington in strictly regulating the collection, use, and storage of biometric information.

The Louisiana Attorney General is the primary enforcer of the Database Security Breach Notification Law. That said, violations of this law also constitute an unfair act or practice pursuant to the state's unfair and deceptive acts and practices law,[71] which is generally enforceable by the Louisiana Attorney General, with a limited private right of action that does not allow for class action litigation.[72] Separately, there is a private right of action under the Database Security Breach Notification Law available in the event of a company's failure to disclose a breach, but only if the breach results in actual damages.[73]

e. Maryland

In May 2020, Maryland enacted legislation that requires companies to obtain consent prior to collecting facial recognition scans of job candidates during the interview process.[74] The law, which goes into effect in October 2020, specifically prohibits potential employers from using a "facial recognition service" to create an interviewee's facial template without prior consent. Facial template is defined as "the machine-interpretable pattern of facial features that is extracted from one or more images of an individual by a facial recognition service."

f. New York

In March 2020, New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) went into full effect.[75] The law updates and expands New York's data breach notification rules and imposes data security requirements with respect to personal information belonging to New York residents. The SHIELD Act includes biometrics in its definition of protected personal information. The SHIELD Act requires companies to implement administrative, technical, and physical safeguards to protect covered information belonging to New York residents and can apply to companies beyond New York's borders. Notably, compliance with HIPAA alone will not exempt covered entities from complying with the SHIELD Act's notice requirements in the event of a breach. Only the New York Attorney General may seek civil penalties for violations of the SHIELD Act.

g. Oregon

The state amended the Oregon Consumer Information Protection Act (OCIPA) effective January 1, 2020.[76] The definition of personal information now includes "[d]ata from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction."[77] Entities covered by HIPAA or the GLBA are exempt.[78] The Oregon Director of the Department of Consumer and Banking Services has investigatory and enforcement powers under OCIPA, which extend outside the borders of the state. Violators are subject to financial penalties.[79]

Importantly, violations of OCIPA are also subject to Oregon's unfair and deceptive acts and practices law,[80] which provides for a private right of action (including class actions), but only if the affected consumer suffers an ascertainable loss.[81]

Other state and federal activity

There are a few sector-specific federal laws that include biometric information in their protections,[82] as well as industry-specific guidance.[83] In 2012, the FTC issued a Staff Report titled "Best Practices for Common Use of Facial Recognition Technologies." Although companies are not bound by these Best Practices,[84] the FTC has, on occasion, exercised its authority under Section 5 of the FTC Act to investigate privacy-related issues, including those arising from facial recognition technology. Further, FTC complaints have been filed against companies in the IoT and AI sectors, alleging that the companies were engaging in deceptive acts or practices in or affecting commerce.[85]

For an example at the state level, the Vermont Attorney General sought an injunction against Clearview AI arising from that company's alleged practice of collecting images of Vermont residents and using artificial intelligence to create "maps" (*i.e.*, templates) of their faces without their knowledge or consent.[86] The complaint, filed in March 2020, alleges violations of the Vermont Consumer Protection Law and its Fraudulent Acquisition of Data Law.[87]

What looms on the horizon?

Federal privacy laws have been proposed in the US Congress, including legislation that would specifically address the commercial use of facial recognition technology and other biometrics.[88] To date, none of these proposed laws has gained traction, leaving the federal government well behind many states on consumer privacy legislation. There have also been sporadic calls for other forms of federal government regulation, such as the creation of an overarching federal agency modeled after the Food and Drug Administration to govern facial recognition technology.[89]

It is only a matter of time before more states join Illinois, Texas, and Washington in strictly regulating the collection, use, and storage of biometric information, as several states have recently considered similar statutes.[90] It is also possible that state attorneys general will scrutinize the area more closely, and plaintiffs' attorneys will likely explore the use of unfair or deceptive acts or practices laws to bring claims against companies for alleged biometrics-related violations of state privacy laws.

The adoption of biometric technology may also give rise to more traditional claims and theories of liability. Most obviously, a breach of biometric data could lead to class action liability, as it has in the case of breaches exposing other types of PII.

Additionally, the collection of biometric data from employees may have unforeseen implications beyond statutory law. In a possible sign of things to come, in September 2019, a union filed a complaint against the Metro-North Commuter Railroad Company (MNCR), which runs the New York City subway and regional commuter trains, seeking injunctive relief to prevent the MNCR from requiring its employees to use a new fingerprinting system to log in and out of work.[91] Specifically, the union sought to enjoin the MNCR from implementing its biometric finger scanning system. The crux of the dispute arose from a 2010 New York State Labor Department opinion that stated that only

The adoption of biometric technology may also give rise to more traditional claims and theories of liability.

voluntary fingerprinting of employees is permissible. On the one hand, the MNCR wanted to implement an efficient timekeeping system that would, in part, curtail overtime cheating. On the other hand, the employees did not want their fingerprints to be used for other purposes, such as criminal background checks. These underlying and conflicting interests are typical in the context of implementing biometrics in the workplace.

Additional litigation or regulatory risk may arise from allegations that facial recognition technology has enabled or masked discrimination against classes of people protected by federal laws based on personal characteristics such as age, sex, race, or disability. For example, if a company were to use biometric data collected for one purpose in making determinations that subject such protected persons to discriminatory practices, that company could face a federal class action lawsuit. As a related issue, improper use of facial recognition technology could give rise to a host of constitutional concerns.[92] This risk highlights what was discussed earlier, vis-à-vis both bias and mission creep.

Conclusion

Although more states – and perhaps the federal government – will enact statutes governing biometrics in the years to come, the legal landscape for companies using biometrics in the United States today is far from settled. This can be a frustrating scenario given that the use of biometrics will only increase. In this time of uncertainty, it is incumbent on private entities to take a commonsense approach as to how they are collecting, using, and destroying biometric data. This includes, for example, understanding what information a company possesses, whether it qualifies as "biometric information" under applicable law, where it is stored, in what format it is stored, how long it is stored, and what security measures are in place during retention and destruction. It is also worth considering for what purpose the information was collected, whether that purpose has evolved over time, and to what extent the owner of the information consented to or was notified of those purposes.

By keeping abreast of legal developments such as those discussed above while taking a clear-eyed approach to their current practices, companies can mitigate their legal risk and take advantage of the numerous benefits biometric technology offers.

Endnotes

1 A handful of municipalities in different states have proposed and passed legislation pertaining to governmental use of facial recognition technology. Those topics are not covered here.

2 According to a recent study by the RAND Corporation, conducted at the behest of the Department of Homeland Security, facial recognition technology used to verify an individual's identity with that person's consent is more accurate and more secure than technology used to identify an individual where consent is not obtained. Douglas Yeung et al., *Face Recognition Technologies: Designing Systems that Protect Privacy and Prevent Bias*, 2020 RAND Corp. 7-8.

3 Under a third scenario, "N:N Identification," there are any number ("N") of templates contained on a system used, for example, as part of a governmental surveillance program. Any number of people can subsequently have their facial image ("N") scanned, such as via closed caption television in a public place, and those facial images can be compared with the templates in order to identify each of the individuals in the crowd, ostensibly for security purposes.

4 Zolan Kanno-Youngs & David E. Sanger, *Border Agency's Images of Travelers Stolen in Hack*, N.Y. Times (June 10, 2019), https://www.nytimes.com/2019/06/10/us/politics/customs-data-breach.html; Julie Hirschfeld Davis, Hacking of Government Computers Exposed 21.5 Million People, N.Y. Times (July 9, 2015), https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html.

5 Patrick Grother et al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, 2019 Nat'l Inst. of Sci. & Tech. 14; *see also* Patrick Grother et al., *Ongoing Face Recognition Vendor Test (FRVT) Part 5: Face Image Quality Assessment*, 2020 Nat'l Inst. of Sci. & Tech. 6 (for public comment) (noting "increased error rates in applications where photography of faces is difficult or when stringent thresholds must be applied to recognition outcomes to reduce false positives").

6 *See Cothron v. White Castle Sys., Inc.*, No. 1:19-cv-00382 (N.D. Ill. removed from Circuit Court of Cook County Jan. 18, 2019).

7 *See Vo v. VSP Retail Dev. Holding, Inc.*, No. 1:19-cv-07187 (N.D. Ill. 2019), *appeal docketed*, No. 20-1684 (7th Cir. Apr. 24, 2020).

8 *See Mutnick v. Clearview AI Inc.*, 1:20-cv-00512 (N.D. Ill. filed Jan. 22, 2020).

9 *See P.S. v. TikTok, Inc.*, No. 5:20-cv-02992-LHK (N.D. Cal. filed Apr. 30, 2020).

10 740 Ill. Comp. Stat. 14/20 (2008).

11 One Illinois appellate court affirmed a lower court's finding of coverage in one BIPA class action. *See W. Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc.*, No. 1-19-1834, 2020 WL 1330494, at *9 (Ill. App. Ct. Mar. 20, 2020).

12 740 Ill. Comp. Stat. 14/10 (2008).

13 *Rivera v. Google, Inc.*, 238 F. Supp. 3d 1088, 1095 (N.D. Ill. 2017); *see also Norberg v. Shutterfly, Inc.*, 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015).

14 "Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color." 740 Ill. Comp. Stat. 14/10.

15 *Id.*

16 *See Rivera*, 238 F. Supp. 3d at 1097 ("if Google simply captured and stored the *photographs* and did not measure and generate scans of face geometry, then there would be no violation") (emphasis in original).

17 As one court put it, the law does not "say[], one way or the other, *how* the biometric measurements must be obtained," and "particular biometric identifiers can, in fact, be collected in various ways without altering the fact that the measurements still are biometric identifiers" subject to BIPA's protections. *Id.* at 1095 (emphasis in original). According to that same court, "[t]he bottom line is that a 'biometric identifier' is not the underlying medium itself, or a way of taking measurements, but instead is a set of measurements of a specified physical component (eye, finger, voice, hand, face) used to identify a person." *Id.* at 1096. Therefore, if a private entity uses an individual's biometric measurements contained in a photograph to ultimately identify that individual, it could constitute a "scan of face geometry," one of the biometric identifiers defined in BIPA. To presume that BIPA's "scan of face geometry" biometric identifier would apply only to an in-person scan of an individual's face, as opposed to any scan from which biometric measurements could be taken, would be a higher-risk interpretation, or, in the words of another court, a "narrow" and "problematic" reading of BIPA. *Monroy v. Shutterfly, Inc.*, No. 1:16-cv-10984, 2017 WL 4099846, at *3 (N.D. Ill. Sept. 15, 2017).

18 740 Ill. Comp. Stat. 14/10. One Illinois federal court has weighed in on what type of data is and is not within the scope of this exemption. *Vo*, 2020 WL 1445605 at *2. In that case, the defendant's software application scans the user's face geometry and then overlays digital eyewear on the scan, allowing the user to remotely "try on" both prescription and nonprescription glasses. The plaintiff alleged that the software collected her biometric data when she used it in Illinois, in violation of BIPA notification requirements. Taking into consideration the HIPAA definition of "healthcare," the court dismissed the plaintiff's claims and held that the defendant's biometric data collection software fell within the scope of the exemption. The software offered both prescription eyewear and replicated services that would typically be performed by an eye care professional, and thus the defendant "collected biometric information from a patient in a health care setting" akin to an initial medical evaluation. BIPA also cannot conflict with the X-Ray Retention Act, or the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004. 740 Ill. Comp. Stat. 14/25 (2008).

19 The exemption for governmental entities extends to contractors and subcontractors.

20 740 Ill. Comp. Stat. 14/25.

21 740 Ill. Comp. Stat. 14/15.

22 A critical point of ambiguity in the law is whether, as a practical matter, its notice and consent requirements can apply equally to those that collect biometric information and to those that receive it. The provisions of Section 15 are not phrased in the passive voice such that a processor or service provider would merely have to ensure, via contract with the collector, that appropriate consent has been obtained. Instead, there is a question as to whether the company itself must inform the individual and collect the individual's written consent. Plaintiffs have seized on the broad provision to assert BIPA violations against third-party vendors that may store or use biometric data despite not necessarily interfacing directly with individuals from whom the biometric data is collected.

23 740 Ill. Comp. Stat. 14/10.

24 740 Ill. Comp. Stat. 14/15.

25 *Id.*

26 *Id.*

27 Article III grants federal courts the power to hear cases and controversies and limits the matters over which federal courts may preside. US Const., art. III, § 2. The US Supreme Court has interpreted Article III to require that plaintiffs suffer an actual or concrete injury in fact in order to seek redress in federal court. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547-48 (2016); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). As a constitutional requirement, plaintiffs must therefore demonstrate an injury that is particularized and that affected them personally in order to bring suit in federal court. *Spokeo*, 136 S. Ct. at 1548 (quoting *Lujan*, 504 U.S. at 560 n.1). The injury must also be real rather than merely abstract, hypothetical, or conjectural. Id.

28 *See Aguilar v. Rexnord LLC*, No. 17-CV-9019, 2018 WL 3239715, at *3-4 (N.D. Ill. July 3, 2018) (finding lack of standing due to absence of concrete harm where employee knew his biometric information was being collected to clock in and out), *rev'd*, 958 F.3d 617, 626-27 (7th Cir. 2020) (declining to find standing with respect to alleged violation of BIPA Section 15(a), but finding standing with respect to BIPA Section 15(b) allegation); *McCullough v. Smarte Carte, Inc.*, No. 16-C-03777, 2016 WL 4077108, at *4 (N.D. Ill. Aug. 1, 2016) (distinguishing BIPA from Article III); *see also Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499, 502 (S.D.N.Y. 2017), *aff'd in part*, 717 F. App'x 12, 18 (2nd Cir. 2017) (affirming lack of Article III standing, but vacating district court's ruling for want of jurisdiction as to the merits of plaintiffs' statutory cause of action).

29 *Monroy*, 2017 WL4099846, at *8 n.5 ("[p]utting aside the question of whether a merely procedural or technical violation of the statute alone is sufficient to confer standing . . ." but finding that the plaintiff's allegation of a privacy violation was sufficient).

30 290 F. Supp. 3d 948, 953-54 (N.D. Cal. 2018), *aff'd*, 932 F.3d 1264 (9th Cir. 2019). In affirming denial of the defendant's motion to dismiss, the Ninth Circuit held that a plaintiff alleging a BIPA violation satisfied the Article III standing requirement because BIPA was designed to protect an individual's common-law right to privacy, which the court found was a concrete (and not merely procedural) injury. This decision was largely at odds with the majority of decisions from district courts in Illinois, which had held, for the most part, that plaintiffs who allege only violation of BIPA's statutory requirements, without some additional harm, do not have standing and may not pursue their claims.

31 First, the violation amounted to an invasion of the plaintiff's "private domain," similar to that of an act of trespass. *Bryant v. Compass Grp. USA, Inc.*, 985 F.3d 617, 624 (7th Cir. 2020). The court further noted that the common interest in protecting individuals' personal privacy bolstered its holding. Second, the court held that the defendant's alleged failure to obtain informed consent from the plaintiff equated to an informational injury, including because the defendant "withheld substantive information to which [the plaintiff] was entitled and thereby deprived her of the ability to give the *informed* consent section 15(b) mandates." *Id.* at 626. Had the plaintiff been provided such information, perhaps she would have made another decision, i.e., to withhold her biometric data from the defendant.

32 *Rosenbach v. Six Flags Entm't. Corp.*, 129 N.E. 3d 1197, 1207 (Ill. 2019); *see also Rottner v. Palm Beach Tan, Inc.*, No. 1-18-0691, 2019 WL 1049107, at *1-2 (Ill. App. Ct. Mar. 4, 2019).

33 Personal jurisdiction is both a statutory and constitutional requirement. States have their own rules regarding what level of activity within the state is sufficient for the court to have personal jurisdiction over the defendant, while the Due Process Clause of the Fourteenth Amendment also requires that the defendant have sufficient contacts with the forum state. *See Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316-17 (1945).

34 *Figueroa v. Kronos Inc.*, No. 19 C 1306, 2020 WL 1848206, at *1-2 (N.D. Ill. Apr. 13, 2020); *Bray v. Lathem Time Co.*, No. 19-3157, 2020 WL 1492742, at *1 (C.D. Ill. Mar. 27, 2020).

35 In one case, the court found that it lacked personal jurisdiction over the defendant, a Georgia-based company with no physical presence in Illinois, and no connection to the state beyond its alleged collection and storage of the plaintiffs' data through the use of its software by the plaintiff's employer. The defendant advertised its products online to residents of Illinois, but the residents to whom it advertised were the third-party employers (the users of the technology), not the plaintiff and members of the proposed class (whose data was collected at the direction of the employers). Moreover, the court noted that the plaintiff's employer purchased the specific device used to collect the plaintiff's biometric data outside of Illinois. *Bray*, 2020 WL 1492742, at *3. This court did not reach the question of whether makers and sellers of timekeeping systems are subject to enforcement actions pursuant to BIPA's private right of action. In the other case, however, the court found that BIPA liability extends to any private entity that obtains biometric information – and that the collection of employees' biometric data by a timekeeping system can create distinct BIPA duties on the part of both the employer and the maker of that system. *Figueroa*, 2020 WL 1848206, at *8. The plaintiffs also alleged that the defendant unlawfully disseminated employee data to other firms, further violating BIPA. Moreover, the defendant sold thousands of timekeeping systems in Illinois, compared with a single system at issue in *Bray*.

36 *See, e.g., Norberg*, 152 F. Supp. 3d at 1105 (denying motion to dismiss for lack of personal jurisdiction).

37 On another note, the *Figueroa* court decision leaves open the question of whether plaintiffs have an actionable injury for purposes of standing where they were unaware they were interacting with the defendant company as a result of the defendant company's failure to notify them.

38 *Rivera*, 238 F. Supp. 3d at 1100; *see also Monroy*, 2017 WL 4099846, at *6.

39 *Monroy*, 2017 WL 4099846, at *6.

40 *Id.* (allowing extraterritoriality defense to be raised at a later time, "if and when the record affords a clearer picture of the circumstances relating to [the plaintiff's] claim").

41 *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 326 n.1 (1989).

42 Another potential defense is a constitutional due process challenge based on the high statutory damages available under BIPA. In a BIPA class action, damages can reach into the millions, if not billions, of dollars, which arguably bears no relation to the minimal harm typically alleged by plaintiffs.

43 *Monroy*, 2017 WL 4099846, at *7-8.

44 In *Peatry v. Bimbo Bakeries USA, Inc.*, No. 19 C 2942, 2020 WL 919202, at *1 (N.D. Ill. Feb. 26, 2020), the court dismissed a portion of the alleged class claims that arose during a time period covered by a collective bargaining agreement to which the plaintiff was subject. *See also Miller v. Sw. Airlines Co.*, 926 F.3d 898, 901 (7th Cir. 2019) (considering preemption under the Railway Labor Act).

45 *See, e.g., Treadwell v. Power Sols. Int'l, Inc.*, 427 F. Supp. 3d 984, 989 (N.D. Ill. 2019) (considering preemptive effect of Illinois Workers Compensation Act with respect to nonphysical and non-psychological injuries alleged in BIPA complaint).

46 735 Ill. Comp. Stat. 5/13-201 (1982), which provides a one-year statute of limitations period, governs "[a]ctions for slander, libel or for publication of matter violating the right to privacy . . . ." One court has found that the "publication" requirement of Section 201 would not apply to BIPA Section (a) and Section (b), but could apply to Section (d), which governs dissemination of biometric information. *Meegan v. NFI Indus., Inc.*, No. 20 C 465, 2020 WL 3000281, *2-3 (N.D. Ill. June 4, 2020).

47 735 Ill. Comp. Stat. 5/13-202 (2016), which provides a two-year statute of limitations period, governs "[a]ctions for damages for an injury to a person . . . or for a statutory penalty . . . ." One court has found that the two-year statute of limitations would not apply to BIPA Section (b) because BIPA is remedial in nature and does not impose statutory penalties. *Meegan*, 2020 WL 3000281, at *4.

48 735 Ill. Comp. Stat. 5/13-205 (1982), which provides a five-year statute of limitations period, governs "all civil actions not otherwise provided for . . . ." One Illinois state court has found that this statute of limitation period applies to BIPA claims. *Robertson v. Hostmark Hosp. Grp., Inc.*, No. 18-CH-5194, 2019 WL 8640568, at *4 (Ill. Cir. Ct. July 31, 2019); *see also Meegan*, 2020 WL 3000281, at *4 (finding that the five-year statute of limitations applies to at least BIPA Section 14/15(b) claims).

49 *Meegan*, 2020 WL 3000281, at *2.

50 Under Rule 23 of the Federal Rules of Civil Procedure, a claim may proceed as a class action only if the class is so numerous that it would be impracticable to join each individual class member to the case separately; there are common issues to the class members; the claims or defenses of the class representatives are typical of those of the class; and the representatives will protect the class interests.

51 TEX BUS. & COM. Code Ann. § 503.001 (West 2019).

52 Some limited exceptions apply. *See* § 503.001(c-1).

53 Wash. Rev. Code § 19.375.900 (2017).

54 *Id.* § 19.86.080.

55 *See* Colorado (Colo. Rev. Stat. Ann. § 6-1-716 (West 2020)); Delaware (Del. Code Ann. tit. 6, § 12B-101 (West 2019-2020); Iowa (Iowa Code § 715C.1 (2018)); Kentucky (KY. REV. Stat. Ann. § 365.732 (West 2020)); Nebraska (Neb. Rev. Stat. § 87-802 (2016)); New Mexico (N.M. Stat. Ann. § 57-12C-2 (West 2020)); South Dakota (S.D. Codified Laws § 22-40-9 (2020)); Wisconsin (Wis. Stat. § 134.98 (2008)); Wyoming (Wyo. Stat. Ann. § 40-12-501 (West 2020)).

56 Ariz. Rev. Stat. Ann. §§ 18-551, 552 (2020).

57 *Arizona's Data-Breach Notification Law* FAQ, Ariz. Att'y Gen. Mark Brnovich, https://www.azag.gov/consumer/data-breach/faq (last visited July 8, 2020).

58 The Arizona Attorney General's enforcement power arises from the Consumer Fraud Act, Ariz. Rev. Stat. Ann. § 44-1521, *et seq.* (2020).

59 Ark. Code Ann. § 4-110-103(7)(E)(ii) (West 2020).

60 *Id.* § 4-110-103(7)(E)(ii)(g).

61 *Id.* § 4-110-105.

62 *Id.* § 4-110-104.

63 *Id.* § 4-110-108.

64 Cal. Civ. Code § 1798.100 *et seq.* (West 2020).

65 *Id.* § 1798(o)(1).

66 *Id.* § 1798.145(a)(5).

67 *Id.* § 1798.150(c) ("Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law.").

68 On February 27, 2020, a California resident and an Illinois resident filed a putative class action against Clearview AI in the US District Court for the Southern District of California.

69 La. Stat. Ann. § 51:3071 *et seq.* (2019).

70 Certain financial institutions are exempt. *See id.* § 51:3076.

71 *Id.* § 51:3074(J); La. Stat. Ann. § 51:1405(A) (2019).

72 La. Stat. Ann. § 51:1409(A).

73 La. Stat. Ann. § 51:3075.

74 H.D. 1202, 2020 Leg., 441st Sess. (Md. 2020).

75 S. S5575B, 2019-20 Leg. Sess. (N.Y. 2019).

76 Or. Rev. Stat. § 646A.600 *et seq.* (2020).

77 *Id.* § 646A.602(12)(a)(v).

78 *Id.* § 646A.604(9).

79 *Id.* § 646A.624.

80 *Id.* § 646A.604(11).

81 Or. Rev. Stat. § 646.638 (2020).

82 *See* Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (protecting student records and personally identifiable information), 34 C.F.R. § 99.3 (defining personally identifiable information to include a biometric record for purposes of FERPA regulations); Genetic Information Nondiscrimination Act of 2008.

83 *Retail Payments Systems Booklet*, Apr. 2016 Fed. Fin. Insts. Exam. Council 33; *Authentication in an Internet Banking Environment*, Oct. 2005 Fed. Fin. Insts. Exam. Council; *Supplement to Authentication in an Internet Banking Environment*, June 2011 Fed. Fin. Insts. Exam. Council.

84 Similarly, the FTC staff issued a Staff Perspective following its joint conference on "Connected Cars" with the National Highway Traffic Safety Administration, in which it noted the risks attendant with connected cars' collection of "sensitive data about the occupants of the vehicle themselves, such as a fingerprint or iris pattern for authentication purposes . . . ." *Connected Cars Workshop: Staff Perspective*, Jan. 2018 Fed. Trade Comm'n 2.

85 *See In re Tapplock, Inc.*, Docket No. C-4718 (May 18, 2020) (FTC announced a settlement with a company that sold biometric-enhanced padlocks that were not as secure as the company touted in its advertising, exposing customer PII to anyone able to access the easily hackable locks); *see also In re HireVue, Inc.* (complaint filed by The Electronic Privacy Information Center with the FTC in November 2019 regarding HireVue's use of AI and biometrics in screening interview technology and failure to meet standards set by the Organization for Economic Co-operation and Development), https://epic.org/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf.

86 *Vermont v. Clearview AI, Inc.* (Vt. Super. Ct. filed Mar. 10, 2020).

87 Vt. Stat. Ann. tit. 9 § 2451 *et seq.*; 9 V.S.A. § 2431.

88 *See, e.g.*, Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (2019); No Biometric Barriers to Housing Act of 2019, S. 2689, 116th Cong. (2019); Ethical Use of Facial Recognition Act, S. 3284, 116th Cong. (2020).

89 *See* Erik Learned-Miller et al., *Facial Recognition Technologies in the Wild: A Call for a Federal Office*, 2020 Algorithmic Justice League 4, 14.

90 Including Alaska, Arizona, Delaware, Florida, Hawaii, Massachusetts, Michigan, Montana, New Hampshire, Rhode Island, and South Carolina.

91 *Ass'n. of Commuter Rail. Emps. Local No. 9 v. Metro-N. Comm. R.R. Co.*, 1:19-CV-08672 (S.D.N.Y. filed Sept. 18, 2019, voluntarily dismissed Feb. 10, 2020).

92 *See* Learned-Miller et al., *supra* note 89, at 11.