

The Sedona Conference Draft Biometric Privacy Primer (April 2022)



The Sedona Conference Draft Biometric Privacy Primer (April 2022)

Drafting Team Members:

Brian Ray (Drafting Team Leader)

Mark Abramowitz

Julian Ackert

Debra Bernard

Melissa Clark

Brett Doran

David Kalat

Colman McCarthy

Frank Nolan

Lesley Weaver

Starr Drum (Steering Committee Liaison)

Ruth Promislow (Steering Committee Liaison)

I. INTRODUCTION

This Primer provides a general introduction to biometric systems, the major legal, policy and practical issues these systems raise, and a summary of existing laws regulating the use of these technologies. As we explain in Part II below, the Primer focuses primarily on biometric recognition systems (which includes both identity verification and identification systems) by private organizations. We focus on biometric recognition systems because these applications are among the most widespread and the most commonly associated with the generic term “biometrics”. While the Primer generally limits its discussion to private-sector applications, it acknowledges—and in several places analyzes—the overlap between public and private applications, including the risks raised by what we term “function creep.”

Audience and Purpose: This Primer is written as a resource for lawyers, judges, legislators, and other policy-makers. It provides a general guide to the relationships among the technical, legal and policy aspects of biometric systems with a particular focus on the privacy and related concerns these systems may raise.

II. OVERVIEW OF BIOMETRIC RECOGNITION SYSTEMS

A. Biometric Modalities and Purpose

Biometrics are generally understood to encompass biological characteristics that make a person unique and allow for identification and/or verification of that individual. Biometric technology records unique physical, factual landmarks of a subject, then later compares a candidate’s similarly acquired landmarks to determine a statistical match likelihood to the original sample.

The public and private use of biometric technology is expanding dramatically. Biometric technologies have become more robust and advanced, substantially reducing error rates through advances in artificial intelligence (AI), including neural networks. As a result, biometrics have developed into a tool for quick and reliable identification or authentication in a broad range of contexts from border control to unlocking smartphones. These techniques are rapidly replacing traditional passwords as a security measure, with newest facial recognition technology enabling the identification in less than one second.¹

The growth of biometric technology is due, in part, to the potential for biometric systems to offer a more secure, faster, simpler and more user-friendly alternative to knowledge-based security systems, such as passwords and physical tokens. This is because biometric systems rely on unique, persistent physical features that, for most applications, a person must physically present to confirm identity.

¹ Soodamani Ramalingam et al., *Fundamentals and Advances in 3D Face Recognition*, in Mohammad S. Obaidat, Issa Traore and Isaac Woungang (eds), *Biometric-Based Physical and Cybersecurity Systems* (2019).

Critics of biometric technologies and academics studying these issues have raised privacy, security and civil liberties concerns in connection with these systems. Some biometric features, such as a person's face, gait, and even fingerprints are difficult or impossible to keep private, which creates the risk that these biometric data can be collected with relative ease and without consent. Even where a person consents to collection, the persistence of biometric features creates heightened concern over unauthorized access and use of that information because the underlying physical characteristic is not easily changed. Well-designed biometric systems convert persistent physical characteristics into proprietary templates that are unusable outside of each system. Yet some privacy advocates, such as the Electronic Frontier Foundation, have voiced concerns that government and law enforcement collection could use biometric information to track a person across multiple systems.²

Some state and local governments, as well as private organizations, have implemented regulatory and policy responses and proposals to try to find a balance that protects individual rights while allowing for the use and growth of biometric technology given its many benefits. For example, some local governments have banned any police use of facial recognition technology, and others have adopted ordinances restricting both private and public use of some biometrics for surveillance.³ Several states have taken up biometric privacy legislation, and industry groups are increasingly advocating for best practices guidelines and other forms of self-regulation.⁴

B. Biometric Recognition Systems Overview

The term “biometrics” is used across multiple disciplines to describe an array of technologies and processes ranging from identity systems to biological processes. The data privacy and related laws discussed in Section IV likewise include different definitions of the term.⁵

For purposes of this overview, we focus on a set of technologies related to identifying individuals that fit the International Standards Organization's definition for biometric recognition: “automated recognition of individuals based on their biological and behavioral characteristics.”⁶ This definition encompasses the two most common biometric processes: biometric verification (sometimes called “authentication”) and biometric identification.

Verification compares an existing template of a biometric identifier to a newly submitted template to verify a person's identity, for example using a finger scan or face template to unlock a mobile phone, or clock into one's workplace. This process is referred to as 1:1 matching

² See, e.g., commentary by the Electronic Frontier Foundation, accessible at <https://www EFF.org/issues/biometrics>; Ann Cavoukian, et al., *Privacy and Biometrics for Authentication Purposes: A Discussion of Untraceable Biometrics and Biometric Encryption*, Int'l Conf. on Ethics and Policy of Biometrics (2010) 14, 14-15.

³ See Section ___ below.

⁴ See Section ___ below.

⁵ See Section ___ below.

⁶ ISO/IEC 2382-37:2017 Information technology — Vocabulary — Part 37: Biometrics, available at <https://standards.iso.org/ittf/PubliclyAvailableStandards/>.

because the software compares the newly submitted information only with the stored information of the claimed identity.

Identification compares a newly acquired biometric template to a database of stored templates to identify an unknown person. This process is used to prevent and detect alias or duplicate enrollments, whether accidental or intentional, called “scrubbing” for double identity holders, and by law enforcement to search for matches against criminal databases for background checks or in criminal investigations, among others.⁷ Private commercial entities have similarly used facial recognition systems to identify individuals accused of prior shoplifting and premium customers.⁸

Most biometric recognition systems follow a basic operating model that includes the following components:

Acquisition and Enrollment: software captures a raw data sample of a particular physical feature from an individual. Some biometric modalities typically require direct contact with a device in order to scan the feature, for example fingerscans capture a 2D image of the friction ridges present on the subject’s finger pad. Others, such as facial recognition, can be acquired from a distance or using existing other sources, such as government ID or even social media postings and other publicly available photographs.

Data Extraction: the software then uses an algorithm to convert the raw sample into a digital biometric template that is usually a mathematical or symbolic representation of the raw sample recording the unique landmarks derived from the subject’s sample. This enables the software to associate that template with an identifier, and then to store it in a database of templates. In some cases, such as a digital eID, the record is placed on a phone or smartcard and is carried by the subject.

Alias/Duplicate Check: where an enrollment database is used, the operator may search that database for potential matches at enrollment to determine if the enrollment is unique. This is one example of the use of 1:n matching for the purposes of creating a 1:1 verification system.

Data Storage: the system retains a database of enrolled templates to search and compare, or the subject may carry their template in a secure form.

Data Matching: software uses a computer algorithm to determine whether the new template matches an existing template(s) from the database or a personally carried medium.

⁷ Due to the complexity of additional issues that arise in the context of law enforcement and national security, this Primer focuses on the use of biometrics in private and commercial applications.

⁸ See Tom Chivers, “Facial recognition... coming to a supermarket near you,” The Guardian, Aug. 4, 2019, at <https://www.theguardian.com/technology/2019/aug/04/facial-recognition-supermarket-facewatch-ai-artificial-intelligence-civil-liberties>.

System Parameters: most systems allow the end-user/operator to define the parameters for when a new sample potentially “matches” the existing record or records.

C. Common Biometric Modalities

Finger Scan

The science of forensic fingerprint analysis was codified by Sir Francis Galton in the late nineteenth century, culminating in the 1892 publication of his landmark treatise *Finger Prints*. Galton cataloged unique characteristics, collectively called “minutia,” that collectively represented the various ridges and valleys that arches, loops, whorls, islands, lakes, and other types of structures evident in a person’s fingerprint. To systematize the process of fingerprint analysis into something that can be performed efficiently by software, modern computerized systems eschew the identification of nearly all of the various structures altogether, and do not attempt to perform pattern matching on images. Instead, most commercial fingerprint-based authentication systems rely on mapping only one type of “minutia.” Although fingerprint analysts have identified as many as 150 different types of minutia, only the points where ridges either terminate or bifurcate are considered salient for the purposes of automated recognition systems.

During the enrollment phase a subject places her finger onto a scanning device. Different manufacturers use a variety of competing sensor technologies including optical, capacitance, pressure, thermal, or ultrasound. Whatever sensor technology is used generates an image of the fingerprint, but this needs to be processed before it can be used to identify minutiae points. First, the grayscale image is converted to a pure black-and-white image with no intermediate grays and is “thinned” to reduce each ridge down to the width of a single pixel. The system then identifies minutiae points by their orientation and coordinates on an x/y plane.⁹ This coordinate information is stored as a “template” and is assigned to a particular user identity or account in the system in question.

During the matching phase, a subject presents her finger to a scanning device to be processed in the same way, and the resulting template is compared to the stored template to determine statistical similarity. If a sufficient number of data points are found in common, the scans are considered to match.

Research has shown that it is unlikely, if not impossible, to achieve a perfect match. The same finger placed on a sensor a hundred times in succession can produce a hundred distinct templates. Consequently, matching algorithms are designed to compare the similarities between the enrolled template and the one presented for authentication. The threshold of similarity can be calibrated by the system designer to balance the risks of false rejection and false acceptance to find the optimum balance of accuracy for the specific use case involved.

⁹ Wieclaw, “A minutiae-based matching algorithms in fingerprint recognition systems,” *Journal of Medical Informatics & Technologies* Vol. 13 (2009); also Ravi, et al., “Fingerprint Recognition Using Minutia Score Matching,” *International Journal of Engineering Science and Technology* Vol. 1(2) (2009).

Facial Recognition

Generally speaking, facial recognition technologies can be sub-divided into two distinct categories, which in turn consist of numerous competing sub-categories. One overall category (Category 1) includes approaches (such as the Principal Component Analysis, or “Eigenfaces,” method) that identify distinguishing relative differences between images within a given set. The second category (Category 2) includes approaches (such as measurements of Facial Geometry) that identify distinguishing features of each subjects’ face. This distinction is important because, generally speaking, the first category of approaches presents a relatively lower risk that the data could be used outside of the specific application than approaches in the second category methods, which create biometric templates that can potentially be used outside the original enrolled setting.

In both categories of facial recognition technology, a visual image of a subject’s face is normalized by some process to identify and extract the facial features relevant to the approach the system uses and store a mathematical representation of the significant features (the “template”). During the matching phase, the same process is repeated and the resulting mathematical representation is compared to the stored template. If a sufficient mathematical similarity (as prescribed by the system owner) is found, the scans are considered to match.

The Category 1 technologies described above are “template”-based approaches that distinguish individual faces from a given, closed, set of data points. By contrast, Category 2 technologies are feature-based approaches that begin with measurements of specific facial features (eyes, nose, mouth, etc.) and their relationship to one another on a given face. Once a prominent orienting facial landmark (typically, the centers of the eyes) is identified, the software crops out non-facial components (such as hairstyle) to isolate the relatively unchanging central features. The software then performs “intensity normalization” to convert certain facial features determined to be useful for discriminating between different faces into numerical vectors.

Iris Recognition

The iris is a thin diaphragm in the middle of the eye, situated behind the cornea and in front of the lens. It is used to regulate the amount of light entering the eye. The iris is composed of a complex set of muscles, tissue, blood vessels, and other biological structures that collectively have a distinct visual appearance. Although it is unknown whether the iris is biologically unique between individuals, it has been found to be distinctive enough for use in biometric systems.

One advantage to using an iris recognition system is that the eye muscles react to light, which enables the scanning system to confirm that the eye is in fact present at the time of scanning (liveness detection), which can guard against the risk of an attacker replaying a recording to the system in place of the actual subject.

Comparing two iris scans is a complex geometric challenge that requires the software to isolate the information describing the biological structures of the iris from the noisy information resulting from how the subject’s head was oriented at the time of the scan, the degree to which

ambient light caused the iris to expand or contract, and other circumstantial differences. In other words, the software must be sophisticated enough to discriminate between the information attributable to the subject's fundamental biology from the information incidental to the circumstances of the scan.

A typical iris recognition system begins by scanning the subject's eye with near infrared light to take several two-dimensional monochromatic images (although the pigmentation of the iris is a distinctive characteristic that humans use to recognize one another's eyes, the color is not relevant to the processing described below and is not retained). The software selects the best of these images and discards the others. The chosen image is then cropped to isolate only the iris from the rest of the image (excluding the pupil, eyelids, eyelashes, and other features). The cropped image is then processed to "unwrap" the conical shape of the iris onto a rectangular shape of fixed dimensions.

The software then encodes coordinates measured from the unwrapped iris, using algorithms to mathematically calculate a binary code called an "iris signature" that contains that coordinate information. This signature is stored as the enrolled template. To authenticate a subject, the same process is repeated to generate a binary iris code to be compared to the template. The comparison uses Hamming Distances to determine the statistical relationship between the two codes.¹⁰

Voice Recognition¹¹

Voice recognition technology proceeds from the assumption that each person's vocal tract is biologically unique, and therefore attributes of the speaker's voice are particular to that tract. The acoustic patterns of the speaker's voice are directly affected by the physical characteristics of the speaker's vocal tract, mouth, nasal cavities, jaw, tongue, larynx, and other biological features.

Unlike the other biometric traits discussed above, the physical features of the speaker's vocal tract are known to change over time, and are affected by the speaker's age, mood, health, and emotional state. Additionally, voice patterns are not as distinctive to an individual as other biometric traits. Nevertheless, there are certain circumstances (such as telephonic communications) where the speaker's voice may be the only feature presented. Consequently, there are situations where voice recognition is the only biometric modality available to authenticate a person's identity.

Voice recognition technology can be "Text Dependent" (where the speaker has to say a certain passphrase to be recognized and authenticated) or "Text Independent" (where the speaker

¹⁰ The concept of "Hamming Distance" is a form of error detection used in binary data, used to distinguish errors (such as minor data corruption or noise) from meaningful differences between data points resulting from being different inputs.

¹¹ As discussed in Section IV, the Texas and Washington statutes each use the term "voiceprint" which arguably is not the same as "voice recognition."

can say anything, and the recognition may run in the background of a voice interaction). A typical voice recognition system begins by sampling a section of the speaker's audio and mapping the audio signal's quality, duration, intensity dynamics, and pitch. Depending on the technology used, different statistical state-mapping models are applied to classify the vocal characteristics. The resulting template is a set of vector states representing the characteristic sound forms derived from the audio sample.

During the matching process, the same process described above is repeated on a new audio sample and compared to the enrolled template. The software compares the vector states to determine a statistical likelihood that the two samples come from the same speaker or not.

III. BIOMETRIC SYSTEM BENEFITS AND CONCERNS

A. Benefits

Biometric systems can provide a variety of operational and security benefits across different settings. Most prominently, biometric technology can allow for enhanced security and protection of information, including sensitive personal information through the use of biometric data as an access gateway in place of passwords or personal information (e.g., social security numbers) that can be forgotten, stolen or shared. To realize these benefits designers of biometric recognition systems prioritize characteristics that meet the following criteria:

Robust: characteristics that are relatively unchanging on an individual over time;

Distinctive: characteristics that exhibit significant variation across individuals within the overall population;

Available: all individuals in the population can be expected to have this characteristic;

Accessible: the characteristic can be measured or scanned electronically; and

Acceptable: individuals do not generally object to having it measured or scanned.¹²

As a consequence of these requirements, only biological or behavioral characteristics that cannot easily be changed are useful for biometric recognition systems. Compared to alternative methods to verify identity, these features can increase both the convenience and security of the recognition process for the following reasons.

The growth of biometric technology is due, in part, to the potential for biometric systems to provide more secure, faster, cheaper, simpler, frictionless, and more user-friendly alternatives to other forms of information security. The central tenets of information security are confidentiality, integrity, and availability (CIA). Proper authentication is needed to proactively ensure that a user is granted efficient and unrestricted access only to the resources s/he is

¹² Wayman, Jain, Maltoni, and Maio (Eds), *Biometric Systems: Technology, Design and Performance Evaluation* (2005), pp. 3-4.

authorized to use, while prohibiting unauthorized access to resources. In the event of a breach or other instance of unauthorized access, the authentication of the user is needed to reactively investigate the cause.

In “real world” scenarios, humans routinely rely on biological features to identify one another. Known associates can be recognized in one-on-one interactions by face or voice, while government issued identification cards provide photographs to facilitate the official verification of one’s identity to a stranger. The use of biometric technology provides a mechanism to adapt this process into an electronic realm.

Proponents of biometric identification and authentication technologies note that it offers significant security advantages over other methods of information security. For example, reliance on passwords introduces a range of risks—from the use of weak or easily guessable passwords, to the ease with which passwords can be shared among other users in ways that reduce the security of the overall system and limit the ability to reliably identify individual users. From a security standpoint, biometrics are preferable over passwords because they tie the authentication process directly to the actual subject’s identity, rather than a password or token that can be forgotten, lost, or swapped. The aspects that make biometric-based security more secure are also aligned with ease of use.

Instead of relying on a user to remember and protect many different passwords, the person physically presents their unique, persistent physical features to an electronic system to gain access. Because the templating technology in each system is proprietary, the individual templates derived from persistent biological or behavioral features cannot be easily replicated even with access to a publicly available feature, like a person’s face. Whereas a person who uses the same “password123” in multiple systems is exposed in all of them when that password is leaked, a person who is authenticated into multiple systems with a biometric, depending on the engineering of the affected systems, would not necessarily be exposed in all of them even if a template from one were to be leaked.

B. Concerns

Critics of biometric technologies and academics studying these issues have voiced concerns that the reliable and persistent link to an individual that makes biological characteristics (like face, iris, fingerprint, and voiceprint) useful for biometric recognition also can be viewed as an intrusion into one’s personal space and privacy – and a challenge to the autonomous control of personal information.¹³

Many automated systems, not just biometric ones, collect, use, aggregate, and share data in ways that are often poorly understood or opaque. As a result, even well-designed systems behaving appropriately can give rise to unease among the system’s users. For example, people may feel alarmed when they think that a system or an entity “knows” more about them than they knowingly or intentionally disclosed. Similarly, privacy advocates have raised concerns that

¹³ See, e.g., Joseph Pato, Lynette Millett eds., *Biometric Recognition: Challenges and Opportunities* (2010), 11; Cavoukian, *supra* n. __.

entities that collect biometric data for one purpose may then use or share that data in an unexpected way. Such concerns may be compounded by the reality that some biological features, like a person's face, are often publicly available, potentially facilitating the identification of an individual or the aggregation of their data without the subject's knowledge.

Consequently, some privacy advocates have argued that compromised biometric information from one system could be used to steal a person's identity across multiple systems that rely on the same biometric feature, or that biometric features could be used to combine data about an individual, de-anonymize it, or share it with multiple entities. The following list identifies and briefly explains some of the key privacy and related concerns that have been raised in the collection and use of biometric information.

Persistent Identification. Biometrics are derived from physiological or biological characteristics that are generally immutable and unique to each individual. Critics of biometric systems are therefore concerned that the collection of biometric information for one application could result in a persistent link between that data and a given individual. Such a connection could allow an individual's data to be associated with their actual identity, or could result in an association between data and an individual that is permanent and can never be severed by the user.

This concern is heightened by the risk that a persistent biological characteristic could be aggregated with other sources of personal information to form a more detailed profile of an individual.¹⁴ Any collection of personal information raises this risk. But unlike information linked by a name, a credit card number, or an IP address, for example – where the link to an individual could be broken – the relatively immutable nature of the biological characteristics used in biometric systems raises concerns that the link may be unchangeable, i.e., data will be permanently associated with one's actual identity.

The proliferation of biometric systems in both private and public settings has coincided with rapid advancement in technical capabilities as well as decreasing costs of the hardware and software components. As a result, technology could develop in ways that permit combining more and better biometric data and other information in ways that compromise individual privacy to a greater extent than any single application. It also raises questions about whether biometric technology is being implemented where increased security and identity verification is required, and with the appropriate biometric security and privacy concerns in mind.

Security. Advocates of biometric technologies argue that such systems offer improved security to verify identity because the biological characteristics used are intimately connected to an individual and often must be physically presented for verification. Biometric systems are not, however, immune from compromise.

Biometric systems approximate whether a new template (i.e., biometric input) sufficiently matches the existing one. Attackers can spoof a system by using techniques such as

¹⁴ AI Now, *Regulating Biometrics: Global Approaches and Urgent Questions* (2020), at 7-8.

downloading or printing a person's photo, using a fake silicone fingerprint, or using a 3D mask. Such attacks are known as presentation attacks.¹⁵

Moreover, recent research has demonstrated the possibility of generating both "master prints" and "master faces" that match the partial fingerprints and faces of multiple people and could therefore theoretically give access to a large number of user accounts for multiple individuals.¹⁶ At present, this risk is remote and limited to systems that use multiple enrollments for the same biometric.

The security of stored biometric information is itself a key consideration. If that information has the potential to be used across multiple systems, compromise of it creates a far greater security risk than a compromised password or other identifier that can be changed.

Publicly Accessible Characteristics. Certain biometric information can be collected without the knowledge of the individual. For example, facial recognition or voiceprint technology can be used without the individual's knowledge or consent. Other modalities that generally require direct interaction with the collection device (e.g., fingerprint placed onto a finger scanning device) may still present some risk of capture through indirect means (e.g., lifting a fingerprint from an item touched by the individual) that allow for the covert collection of information.¹⁷

Secondary Information. Templates from some biometric systems could contain secondary information that could be harvested and used beyond the individual's knowledge or consent. For example, some systems claim to be able to detect emotions and other information from both static and live facial images.¹⁸

Tracking and Surveillance. Identifying individuals by means of biometric information expands the ability to track the movement, activity, and behavior of those individuals. This is particularly the case with biometric information that can be implemented surreptitiously – most notably, facial recognition technologies.

Function Creep. Function creep involves the reuse of sensitive information beyond the purpose for which it was originally collected. Function creep can occur with benevolent intent. For example, in Australia, a biometric database originally designed to prevent cross-border criminal activity was used to identify individuals who lost other forms of identification in

¹⁵ See, Abdenour Hadid, Nicholas Evans, Sebastien Marcel, and Julian Fierrez, "Biometrics Systems Under Spoofing Attack: An evaluation methodology and lessons learned," IEEE Signal Processing Magazine, vol. 32, no. 5, pp. 20-30, Sept. 2015, doi: 10.1109/MSP.2015.2437652.

¹⁶ See Aditi Roy, et al., *MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems*, 12 IEEE Transactions on Information Forensics and Security 2013 (2017), at <https://ieeexplore.ieee.org/document/7893784>; Ron Shmelkin, et al., *Generating Master Faces for Dictionary Attacks with a Network-Assisted Latent Space Evolution*, arXiv:2108.01077v3, at <https://arxiv.org/abs/2108.01077>.

¹⁷ See, e.g., Yamila Levalle, *Bypassing Biometric Systems with 3D Printing and 'Enhanced' Grease Attacks*, Dreamlab Technologies (June 2020), at https://dreamlab.net/media/img/blog/2020-08-31-Attacking-Biometric-Systems/WP-Biometrics_v5.pdf.

¹⁸ See, e.g., EDPS, *TechDispatch on Facial Emotion Recognition*, https://edps.europa.eu/system/files/2021-05/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf.

brushfires and provide them aid.¹⁹ But it may also compound potential concerns about identity theft, tracking, the collection or sharing of personal information, and misidentification, particularly as the use of biometrics evolves and becomes more predominant.

Function creep raises issues with whether a person has consented to new and different uses of their biometric information. Someone who has consented to the collection of their biometric identifiers as a secure method for building access at their workplace, for example, may not have provided consent for the use of their biometric information to identify their whereabouts in the building, assess their health, or evaluate their emotional state at work. An individual who has consented to the use of their facial geometry for a mobile application's photo filter may not have consented to the use of that biometric information as a personal identifier.

Function creep also can affect security. Using biometric data for new purposes often means increased access, storage points, and potential disclosure of that data.

Likewise, the quality and integrity of biometric data require examination when function creep arises – the integrity of biometric data suitable for one purpose (e.g., home security) may not be suitable for a new purpose (e.g., criminal identification by law enforcement) and may result in misidentification or security flaws.

The potential for private biometric systems to share information with law enforcement and national security agencies intensifies these concerns. In 2015, the FBI announced that it would start to retain fingerprints submitted for routine background checks in its searchable criminal database.²⁰ A series of U.S. House and Senate investigations into law enforcement access to private biometric databases have highlighted the sometimes blurred lines between private and public use of biometric information and even prompted legislation.²¹ The examples cited in these investigations demonstrate the ease with which private biometric information can be obtained and shared with law enforcement.²²

Discrimination and Bias. Critics of biometric systems and other algorithm-based decision systems have noted patterns of discrimination against certain groups, which can result in

¹⁹<https://www.itnews.com.au/news/services-australia-put-face-matching-to-work-for-bushfire-relief-payments-548978>; <https://www.itnews.com.au/news/australias-new-facial-verification-system-goes-live-441484>

²⁰ <https://www.eff.org/deeplinks/2015/09/little-fanfare-fbi-ramps-biometrics-programs-yet-again-part-1>

²¹ See Sen. Markey, <https://www.markey.senate.gov/news/press-releases/senator-markey-presses-clearview-ai-on-facial-recognition-monitoring-during-nationwide-protests>; Fourth Amendment is Not For Sale Act, S. ___, available at <https://www.wyden.senate.gov/imo/media/doc/The%20Fourth%20Amendment%20Is%20Not%20For%20Sale%20Act%20of%202021%20Bill%20Text.pdf> [update]

²² See, e.g., Sen. Ed Markey, “Senator Markey Investigation into Amazon Ring Doorbell Reveals Egregiously Lax Privacy Policies and Civil Rights Protections,” Nov. 19, 2019, available at, <https://www.markey.senate.gov/news/press-releases/senator-markey-investigation-into-amazon-ring-doorbell-reveals-egregiously-lax-privacy-policies-and-civil-rights-protections> (describing extensive law enforcement access to Ring Doorbell camera footage and an abandoned proposal to incorporate facial recognition into Ring system).

being used to perpetuate and exacerbate existing discriminatory structures or processes.²³ Among biometric modalities, facial recognition has received the most attention in this area because facial features used for identification more often correlate with salient demographic features like race, sex, and age, than other biometric modalities such as fingerprints and irises.²⁴

In spite of the substantial attention that these issues have received, there is no single accepted definition of what constitutes “fairness” for biometric systems (or algorithms more generally).²⁵ From a technical performance perspective, it is relatively straightforward to measure and quantify how a system performs on a specific metric across different demographics.²⁶ For example, the National Institute of Standards and Technology (NIST) has engaged in ongoing performance testing comparing several facial recognition algorithms against trained human reviewers. This Facial Recognition Verification Testing, with some notable exceptions, has reported higher error rates for some demographic groups for both verification (1:1 matching) and identification (1:n matching), although the studies indicate that the systems are improving over time.²⁷

The rapid evolution of biometric systems promises eventually to make these systems highly accurate across all demographics. Even where a biometric system meets a set of technical standards for accuracy and non-bias in a test setting, it may exhibit flaws in real-world conditions and/or the testing scenario may fail to adequately consider the operational and social aspects of real-world applications that can introduce inaccuracies or bias.

Transparency. The risk of discrimination is exacerbated by the frequent lack of transparency in the deployment of these systems, and the alleged use of privately created “watch list” databases.²⁸ Individuals often have no way of knowing that a private system has flagged their biometric information (most often facial templates created from surveillance camera

²³ See, e.g., Davide Castelvecchi, “Is facial recognition too biased to be let loose?,” *Nature* (Nov. 18, 2020), at <https://www.nature.com/articles/d41586-020-03186-4>. For a broader discussion of these issues, see Christiane Wendehorst and Yanic Duller, *Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces*, European Parliament, Policy Department for Citizens’ Rights and Constitutional Affairs Directorate-General for Internal Policies Study (Aug. 2021), [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU\(2021\)696968_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf).

²⁴ Christian Rathgeb, et al., *Demographic Fairness in Biometric Systems: What do the Experts say?*, arXiv:2105.14844v1, (May 31, 2021), at 1, available at <https://arxiv.org/pdf/2105.14844.pdf>.

²⁵ *Id.* at 3.

²⁶ *Id.*

²⁷ <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>.

²⁸ See AI Now, *Regulating Biometrics: Global Approaches and Urgent Questions* (2020), at 11; Singh et al., *Biometric Security System for Watchlist Surveillance*, 46 *Procedia Computer Science* 596 (2015).

footage) or any opportunity to contest it.²⁹ This lack of transparency and procedural protections heightens the accuracy and bias risks identified above because many systems are less accurate for people of color and women.³⁰

IV. SYSTEM SELECTION AND DESIGN

The process of selecting or designing biometric recognition systems present organizations the opportunity to make intentional choices about which biometric modality is the right fit for the intended use and how the security of that system is protected. Given the existing uncertainty over key issues in existing laws and the rapidly changing legal landscape summarized in Section IV, when selecting, designing and implementing biometric systems organizations should carefully consider not only existing legal and regulatory requirements but also the potential need to adapt to new laws

Organizations that are considering implementing biometric systems may be able to mitigate the risks to users and to their own organizations by carefully considering the following:

- **Biometric Modality:** Whether a biometric is necessary for the application and the suitability of the biometric for the specific application, including the legal, security and privacy risks it poses relative to other modalities.
- **System Design and Accuracy:** Accuracy depends on the entire system, not only the algorithm used in it.
- **Security and Integrity:** Some biometric modalities are better suited than others to the development of templates that are well protected against reverse engineering the original biological feature.

A. Biometric Modalities

Biometric systems offer different benefits and pose some distinct risks compared to traditional identity verification methods. When deciding whether to use a biometric system by itself or in combination with other recognition methods, it is important to consider whether the distinctive features of biometric systems are suited to the application.

It is equally important to recognize that each biometric modality offers a different mix of benefits and risks. For example, people's faces are a fundamentally public feature, commonly visible and exposed. This fact, coupled with the ability for technology to effectively perform facial recognition on photographs or surveillance video, regardless of whether the subject purposefully engaged in the recognition process, gives rise to a broader range of privacy

²⁹ Meredith Whittaker, Written Testimony, U.S. House of Rep. Cmtee on Oversight and Reform, "Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy," Jan. 15, 2020, at 4, available at <https://ainowinstitute.org/oversight-committee-testimony-whittaker.pdf>; Cavazos, *supra* n. __ at 108.

³⁰ In a recent example, Apple was sued by a black man who was misidentified as a shoplifter by one of its retail store's facial recognition security system. See Kim Hart, "Facial recognition surges in retail stores," Axios, July 19, 2021, available at <https://www.axios.com/facial-recognition-retail-surge-c13ff8d-72c6-400f-b680-6ae2679955d4.html>.

concerns, as detailed in Sedona’s companion publication *Commentary on Notice and Consent Principles for Facial Recognition Technology*.³¹ Those same features, however, also offer distinctive benefits, including the ability to conduct remote identity verification.³²

Biometric systems built around finger scans or iris recognition typically require the active participation of the subject in order to perform any biometric recognition. The addition of “liveness detection” features to such systems can further ensure that the subject is knowingly present as a participant in each biometric recognition event. In addition to being relatively private, irises and fingers are examples of features whose rich biological complexity means that templates can be derived from them that extract only a relatively small fraction of the available biological information. This limited extraction of biological detail can help in designing templates that cannot be usefully repurposed outside of the original system.

B. System Design and Accuracy

In general, organizations that are selecting or designing biometric recognition systems should consider how best to protect individual privacy when the biometric data is collected from subjects, when the biometric data is used for its intended purpose, and at any subsequent decision point when new purposes are considered. Each of these steps represent distinct moments of risk, and may have different answers. For example, an organization that is collecting biometric data carefully and responsibly, and using it for an appropriate purpose, may find that subsequent re-use of the same data may implicate new privacy concerns or dangers.

The accuracy of each biometric system varies significantly depending on what aspect of system performance you intend to measure. For example, a system may perform well when measuring the overall percentage of correct identifications but poorly when measuring its ability to correctly identify a single individual across multiple different photos. Accuracy also depends on how a system is configured and actually used in a specific application.³³

The following list identifies and briefly describes the most significant factors that can affect the accuracy of biometric systems. These factors operate together to determine the accuracy of a given biometric system.

Input Image Quality: the quality of the input (such as an image, or audio) used to create the biometric template at the enrollment phase and of the probe data or image used to verify or identify a person directly affects the accuracy of the system. For example, a face recognition system that requires a subject to position their face within a prescribed zone on a high-definition camera will have a higher accuracy than one based on low-resolution surveillance video.

³¹ See Sedona Conference *Commentary on Notice and Consent Principles for Facial Recognition Technology*

³² See Section II above.

³³ Generally speaking, the accuracy of biometric systems using the most commonly modalities of fingerprint, face and iris have improved dramatically during the last several years, with several facial recognition systems performing more accurately than trained human reviewers in the ongoing Facial Recognition Verification Testing (FRVT) program conducted by the National Institute of Standards and Technology (NIST). See <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>.

Aging: some biometric characteristics (most notably facial features but also voice) change over time, reducing the accuracy of the system.

Algorithm Architecture and Training Data: the accuracy of algorithms used across different biometric systems can vary significantly and can be influenced by the quality, quantity and diversity of the data used to train the system. As discussed, different demographic groups may experience different rates of accuracy from the same systems and algorithms.

Skill/Training/Experience of Human Examiner: in systems where a human is involved in the process, the skill, training, and experience (including implicit biases) of each individual examiner can strongly influence the results and either reduce or increase the overall accuracy.

Search Parameters: biometric systems often permit users to define the parameters of the search in ways that can influence accuracy by, for example, calibrating the system to require a relatively closer match to the probe image or, conversely, in 1:n identification systems requiring that the system return a set number of matches regardless of confidence level.

One basic measure of the accuracy of a biometric system focuses on is the rate of false matches (“false positives”) and the rate of false non-matches (“false negatives”). Each time a system captures a person’s biometric the resulting template will be slightly different. The algorithm used in the data matching process therefore must estimate whether the new template is sufficiently similar to the stored one. Generally speaking, this means that calibrating a system’s algorithm to accept a greater range of variability in the new template to reduce the number of false negatives will increase the number of false positives, and vice versa. The desired balance will vary depending on the specific technology and its individual implementation. For example, configuring a system to prioritize efficiency and access requires accepting a larger number of false positive identifications by permitting the system to accept a larger variation in templates. By contrast, prioritizing security requires accepting a larger number of false negatives to ensure that the system accepts only very closely matched templates.³⁴

The ISO recognizes three kinds of biometric system evaluations. Technology, Scenario, and Operational. NIST evaluations have documented increasing accuracy on technical evaluations for the top-performing systems in major modalities but also substantial differences among systems.³⁵ Scenario and Operational testing are less common but important to identify how systems work under the actual conditions in which a system operates. Even systems that incorporate algorithms that perform well under NIST’s technical evaluations may perform less well in real-world conditions.³⁶ Independent scenario and operational testing of facial recognition systems has demonstrated that accuracy depends on the entire system configuration,

³⁴ See National Cyber Security Centre, “Biometric recognition and authentication systems: Measuring performance,” Version 1.0 (Jan. 24, 2019), at <https://www.ncsc.gov.uk/collection/biometrics/measuring-performance>

³⁵ See <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>

³⁶ See Y.B. Sirotnin, A.R. Vemury. Demographic Variation in the Performance of Biometric Systems: Insights Gained from Large-Scale Scenario Testing. In Virtual Events Series- Demographic Fairness in Biometric Systems. EAB, 2021.

including the quality of the equipment used to acquire images and the conditions under which they were created.³⁷

C. Security and Integrity

Well-designed biometric systems emphasize process integrity as much as secrecy to ensure that the chain of custody from sample capture, comparison, and returning results are protected from tampering or manipulation even by an imposter armed with stolen or publicly captured biometric data. The protection of biometric data is traditionally judged according to the following principles:³⁸

Security: It should be computationally infeasible to reverse a protected template back to the original biometric characteristic; well-designed systems use proprietary templates and algorithms that are not interoperable across systems.

Diversity: If the protected template is obtained by an attacker, it should be impossible to use it in a different database or system;

Revocability: If a protected template is compromised, it should be straightforward to revoke it and replace it with a new protected template based on the same biometric characteristic;

Performance: The protection scheme used to achieve the previous three principles should not materially degrade the system's false acceptance or false rejection rates.

Data security for a biometric system should be designed appropriately to account for both the algorithm used to create protected templates as well as the new and existing or enrolled protected templates. The following aspects of data security should be included, focusing on a security posture that segregates the algorithm from the protected templates as the risk of a security incident that discloses identities is lowered if only one aspect (either the algorithm or the protected templates) of the biometric system is compromised.

For the algorithm used to create protected templates, security measures should protect against both the exfiltration and/or the modification of the algorithm. This includes, but is not limited to, use of encrypted storage best practices, the implementation of appropriate access control that leverages multi-factor authentication, and the monitoring of accesses such as views and/or downloads. Additionally, the algorithm itself should be designed in a way such that it holds no value outside of the current system. This ensures that if the algorithm is exfiltrated from one system, it cannot be used to reverse engineer the biometric attributes of templates from another system.

³⁷ See Yevgeny Sirotin, 'Bias' in face recognition: some facts, LinkedIn, Oct. 16, 2019 at <https://www.linkedin.com/pulse/bias-face-recognition-some-facts-yevgeniy-sirotin-phd/>.

³⁸ Jain, Ross, and Nadakumar, Introduction to Biometrics (Springer, 2011), pp. 286-287.

For the new and existing or enrolled templates, security measures should protect against the injection of unauthorized templates. This includes, but is not limited to, use of encrypted storage best practices, the implementation of appropriate access control that leverages multi-factor authentication, and the monitoring of accesses such as views and/or downloads. Additionally, there should be a method by which a template can be validated against the algorithm of the specific biometric system that was used to create the template. This ensures that if an unauthorized template is injected into the biometric system, it cannot be used to validate unauthorized credentials as the injected template would not validate against the specific biometric system algorithm. Note that if biometric system algorithms are designed such that they are proprietary to a given system and dissimilar to other system algorithms, then exfiltration of a protected template itself has no value outside of the existing system and cannot be used on its own to reverse engineer the biometric attributes of an individual.

Data integrity principles should be integrated into the design of a biometric system. Data security and data integrity are intertwined – data integrity follows appropriate data security. Specifically, there should be a focus of the following key elements of data integrity between the algorithm and the protected templates.

There should be appropriate chain of custody and data validation steps such as checksums when protected templates are created. Data integrity implemented at the time of protected template creation ensures that templates are not useful outside of their biometric systems, and therefore cannot be used to reverse engineer the specific biometric data points used to create the template without the corresponding algorithm. Data integrity can affect system accuracy, specifically as it relates to the balance between false positives and false negatives, which is dependent on the use of the biometric system (verification, or 1:1 matching, vs identification, or 1:n matching).

IV. U.S. BIOMETRIC PRIVACY LEGAL LANDSCAPE

A. Overview

As recently as 2019, there were only three states with laws specifically regulating biometric technologies: Illinois, Texas and Washington.³⁹ Recently, several other states have joined that small group⁴⁰ and most of the growing number of state consumer data privacy laws also protect biometric information.⁴¹ Several other states have amended their data protection and breach notification laws to include biometric information.⁴²

³⁹ See Section IV.B for a detailed analysis of the current U.S. biometric privacy laws.

⁴⁰ See, e.g., Ark. Code § 4-110-104, Cal. Civ. Code § 1798.100.

⁴¹ See e.g., COLO. REV. STAT. ANN. §§ 6-1-713, 6-1-713.5; MD. CODE ANN., COM. LAW §§ 14-3501 *et seq.* Virginia's Consumer Data Protection Act, which comes into force in 2023, similarly includes consent and related obligations for collecting biometric information.

⁴² See e.g., Ark. Code Ann. §§ 4-110-101 *et seq.*; Del. Code Ann. tit. 6, §§ 12B-101 to 12B-1049; Iowa Code Ann. § 715C.1-2; 9 Vt. Stat. §§ 2430 to 2445; Wis. Stat. Ann. § 134.98.

At the federal level, there have been several unsuccessful legislative proposals to regulate biometric privacy.⁴³ The Federal Trade Commission’s general consumer protection authority over data privacy and security encompasses biometric information, and following its first enforcement action in this area, the FTC has signaled that it will continue to scrutinize facial recognition technology.⁴⁴ Sector-specific laws, most prominently HIPAA, also regulate some biometric information and/or practices related to that information.⁴⁵

Government acquisition and use of biometric information is governed broadly by federal law and, at the state and local levels, a growing number of ordinances regulate the acquisition of surveillance technologies and, more recently, ban the use of facial recognition. Recent proposals to expand the use of biometric systems by federal agencies have come under increased scrutiny and reversed in several prominent cases.⁴⁶

The rapid evolution of the legal landscape in this area means that any summary of existing laws risks becoming outdated even before it is published. To date, with the exception of some primarily local and county-level ordinances, U.S. biometric privacy laws do not prohibit the private use of biometric technologies and/or collection, storage and use of biometric information. Instead, these laws impose varying notice, consent and security requirements and limits on sale and reuse of biometric information.

The following summary of existing U.S. state biometric privacy laws highlights the most common requirements and key differences with a focus on the Illinois Biometric Information Privacy Act (“BIPA”). BIPA is the leading model for biometric-specific legislation and, in part because it contains a private right of action, is the most extensively litigated.

B. State Biometric Privacy Laws

1. Biometric/Covered Information Definition

The rapidly evolving nature of biometric technology and the challenges defining “biometric” have led to legal disputes concerning the definition of “biometrics.” Definitions

⁴³ See, e.g., S.2052 Facial Recognition and Biometric Technology Moratorium Act of 2021, 117th Cong. (2021-2022); S.4400 - National Biometric Information Privacy Act of 2020, 116th Cong. (2019-2020).

⁴⁴ *In the Matter of Everalbum and Paravision*, Commission File No. 1923172, <https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3172-everalbum-inc-matter>; *Statement of Commissioner Rohit Chopra In the Matter of Everalbum and Paravision*, Commission File No. 1923172, Jan. 8, 2021, https://www.ftc.gov/system/files/documents/public_statements/1585858/updated_final_chopra_statement_on_everalbum_for_circulation.pdf.

⁴⁵ See 45 C.F.R. 164.512.

⁴⁶ For example, the Internal Revenue Service reversed its decision to require taxpayers to verify their identities using a private facial recognition service and the Department of Homeland Security rescinded a proposal to expand the use of biometric verification systems for people applying for immigration benefits. See Kimberly Adams and Jesus Alvarado, “About-face: IRS to stop using ID.me to identify taxpayers,” Marketplace, Feb. 8, 2022, <https://www.marketplace.org/shows/marketplace-tech/about-face-irs-to-stop-using-id-me-to-identify-taxpayers/>; Sara Hussain, “Victory! Biden Administration Rescinds Dangerous DHS Proposed Rule to Expand Biometrics Collection,” Electronic Frontier Foundation, June 30, 2021, <https://www.eff.org/deeplinks/2021/06/victory-biden-administration-rescinds-dangerous-proposed-rule-expand-biometrics>

under operative and proposed state statutes vary, and litigation has often centered on these questions. For example, BIPA defines biometric “identifiers” as a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry), and defines biometric “information” broadly to include any information based on an individual’s biometric identifier that is used to identify an individual. The Illinois statute expressly excludes certain data elements from the definition of biometric “identifiers” or “information” (such writing samples, photographs, tattoo descriptions, information captured in a health care setting or under HIPAA).

How to apply these definitions to newer technologies and different applications – *e.g.*, AI machine-learning systems for facial analysis or recognition which do not use facial geometry, or speech recognition technologies which can understand human speech – and the scope of the exceptions to BIPA is the subject of debate.

California’s law uses a different model. The California Consumer Privacy Act (“CCPA”) defines biometric information broadly based on the ability to extract an identifier template, expressly includes imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template can be extracted (faceprint, a minutiae template, voiceprint), and keystroke patterns, gait patterns, and sleep, health, or exercise data.⁴⁷ This derivative approach extends the law to a newer set of applications that use unique individual traits or behaviors that might not be covered under narrower definitions. It also creates flexibility for the law to encompass future applications.

Competing concerns about ambiguity and clarity in each of these models animate debate not only about effective legislation, but also compliance.

2. Exemptions from Biometric Regulation

Biometric privacy laws may include exemptions for regulated sectors like finance and healthcare that have sector-specific laws regulating the privacy and data security of personal information, including biometrics. Many biometric privacy laws carve out from coverage uses that would otherwise be covered by these sector-specific laws. For instance, BIPA excludes financial institutions or their affiliates that are subject to Title V of the federal Gramm-Leach-Bliley Act, as well as information subject to HIPAA and information collected, used or stored in a health care setting.⁴⁸ Many laws also tend to make exceptions for uses that are pursuant to a valid warrant or subpoena or in court proceedings.⁴⁹

⁴⁷ CCPA, Cal. Civ. Code § 1798.140.

⁴⁸ See 740 ILCS 14/10, 14/25(b), (c). In addition, the Washington law provides for GLBA and HIPAA exemptions, but also carves out uses “in furtherance of a security purpose” and a law enforcement officer acting within the scope of his or her authority. RCW 19.375.020(7), 19.375.040. The Washington law also only applies where the enrollment of the biometric data is for a “commercial purpose.” The exemptions in the Texas law are narrower, only carving out voiceprint data retained by a financial institution or an affiliate of a financial institution under GLBA from the application of the statute. § 503.001(e). The Texas statute also only applies where the data is captured for a “commercial purpose.”

⁴⁹ See 740 ILCS 14/25(a).

3. Notice and Consent Requirements

Most biometric privacy laws require notice and consent prior to use and/or disclosure, or allow consumers to opt out afterwards or from future disclosures. As with any new regulation, there are concerns about compliance with and enforcement of these procedures.⁵⁰

For example, BIPA requires written notice that biometric identifiers or information are being collected and the “specific purpose and length of term” for the collection/use/storage, and the entity collecting the data must obtain a written release prior to their collection or receipt.⁵¹

The CCPA requires businesses to provide individuals with notice that their biometric data is being collected, and whether it is sold or disclosed and to whom. Express consent is not required for collection but individuals must be afforded the ability to opt out or request deletion of their data.

The Washington law requires a “context-dependent” disclosure given “through a procedure reasonably designed to be readily available to affected individuals” prior to enrolling a biometric in a database.⁵² The law specifies that the “exact notice and type of consent required to achieve compliance with subsection (1) of this section is context-dependent,” but is something less than affirmative consent.⁵³ The Washington law also requires consent for new uses or disclosures where a biometric is enrolled or disclosed for a commercial purpose in a manner “that is materially inconsistent with the terms under which the biometric identifier was originally provided.”⁵⁴

4. Sale and Disclosure of Biometric Data

Current and proposed laws address the sale and disclosure of biometric data by prohibiting or restricting the sale or profiting from biometrics as well as placing restrictions on their disclosure. For example, BIPA requires notice and prior consent for any disclosure of biometric data to a third party.⁵⁵ Moreover, BIPA prohibits “private entity[s] in possession of a biometric identifier or biometric information” from selling, leasing, trading, or “otherwise

⁵⁰ Although currently there is no comprehensive federal biometric data privacy law, the Federal Trade Commission recently settled an enforcement action under Section 5 of the Federal Trade Commission Act against a company connected to its use of facial recognition technology. According to the FTC’s complaint, the company violated Section 5’s prohibition of “deceptive acts or practices in or affecting commerce” by allegedly (1) promising to delete users’ images if they deactivated their accounts, but in fact retaining the images and (2) suggesting on its website that it would only apply facial recognition technology to users’ images with users’ consent, but actually enabling the technology by default without many users’ consent.

⁵¹ 740 ILCS 14/15(a).

⁵² RCW 19.375.020(2).

⁵³ *Id.*

⁵⁴ *Id.* at s. 5. The Washington law also permits disclosures for service providers or where a third party contractually promises not to further disclose the biometrics without notice and consent. Cite.

⁵⁵ 740 ILCS 14/15(d); *see also* RCW 19.375.020(3) (permitting disclosure where necessary to provide a product or service explicitly requested by the individual).

profit[ing]” from a person’s biometric identifiers or biometric information.⁵⁶ The scope and application of this provision, however, remains unclear. For example, some argue that a private entity that sells a “biometric device” or hosts such data for a fee are “otherwise profiting” from a person’s biometrics, while others contend such indirect “profiting” not involving the sale of biometric information is outside the scope of BIPA and prohibiting it would substantially curtail or eliminate the ability of companies to provide biometric technology or data hosting.

By contrast, the CCPA permits businesses to sell personal information, including biometric information, but requires notice and a right to opt out.⁵⁷ An opt-out gives consumers the ability to direct a business not to sell their personal information, including biometric information, to a third party, but does not prohibit a business from distributing the data within the organization that collected it (even to different business units). Businesses which receive a request to opt out must stop selling personal information (with some exceptions) and may only request that an individual opt back in after 12 months.⁵⁸

5. Retention of Biometric Data

As discussed in Part III above, biometric data generally is considered personal information that may pose privacy and security concerns when collected and retained. Some biometric laws address retention requirements by imposing an upper limit on the retention period, pegged to the purposes or services for which the biometrics were collected.⁵⁹ Considerations for such laws includes whether there should be exceptions for the specified retention periods (for example, for security, recordkeeping, or law enforcement purposes), what “publicly available” means, and how narrowly to define the initial purposes for the collection.

7. Enforcement and Penalties

Existing biometric privacy laws generally take one of two approaches to enforcement of the statute: (1) providing for a private right of action, and/or (2) enforcement by state attorneys general.

⁵⁶ *Id.* at 14/15(c).

⁵⁷ Cal. Civ. Code § 1798.120.

⁵⁸ *Id.* at § 1798.135.

⁵⁹ For example, BIPA requires the creation of a retention schedule and guidelines for destroying biometrics, both of which must be publicly available and allows for retention until the “initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of the individual’s last interaction with the private entity, whichever occurs first.” 740 ILCS 14/15(a). The Texas law requires retention within a “reasonable period of time” but then caps that period at a year after there is no longer a valid reason for maintaining the biometric. Tex. Bus. & Com. Code Ann. § 503.001(c)(3). Where the biometric serves the purpose of employee identification (“security purposes”), then the biometric must be destroyed within a year after the employment relationship is terminated. *Id.* at § 503.001(c)(3)(c-2). The Washington statute provides that the entity “may retain the biometric identifier no longer than is reasonably necessary to: (i) Comply with a court order, statute, or public records retention schedule specified under federal, state, or local law; (ii) Protect against or prevent actual or potential fraud, criminal activity, claims, security threats, or liability; and (iii) Provide the services for which the biometric identifier was enrolled.” RCW 19.375.020(4)(b)(i)-(iii).

BIPA provides a private right of action, allowing individuals alleging the biometric data was collected, disclosed or retained in violation of BIPA to bring claims in court.⁶⁰ State and federal courts have largely held that mere technical violations of BIPA, with no alleged harm, are sufficient to bring claims. California provides a private right of action limited to the unauthorized access and exfiltration, theft, or disclosure of certain types of personal information, including the right to seek statutory damages.⁶¹ Other states, like Texas and Washington, restrict enforcement to their respective state attorneys general.⁶²

These biometric privacy laws also provide for monetary penalties and other compensation. BIPA provides the greater of a specified liquidated damages penalty or actual damages and distinguishes between negligent and intentional/reckless violations, as well as reasonable attorney's fees and costs.⁶³ Other states provide statutory cap per violation.⁶⁴

8. Security.

The current and proposed biometric privacy laws approach data security by providing a baseline standard for security. For example, BIPA and the Texas law require the storage, transmission, and protection from disclosure “using the reasonable standard of care within the private entity’s industry” and “in a manner that is the same as, or more protective than, the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.”⁶⁵ The Washington law requires only “reasonable care.”⁶⁶

General privacy laws that encompass biometrics also require a baseline level of security, with California’s law permitting private rights of action where a data breach results from a business’ “violation of the duty to implement and maintain reasonable security procedures and practice appropriate to the nature of the information.”⁶⁷

The general trend in data security laws is toward more specific requirements, though there is debate whether that approach is appropriate given the rapidly evolving security threat landscape. For example, the NY Shield Act, which includes “biometric information” in its definition of “private information” regulated under the statute, requires reasonable safeguards to

⁶⁰ 740 ILCS § 14/20.

⁶¹ Cal. Civ. Code § 1798.150.

⁶² Wash. § 503.001(d); Tex. RCW § 19.375.030(2).

⁶³ BIPA provides for the greater of liquidated damages of \$1,000 (negligent violations) or \$5,000 (intentional or reckless violations) or actual damages. 740 ILCS 14/20(1), (2). BIPA also provides for reasonable attorneys’ fees and costs. *Id.* at 740 ILCS 14/20(3).

⁶⁴ Washington caps damages at \$2,000 per violation. RCW § 19.375.030(2); RCW § 19.86.140. Texas caps civil penalties at \$25,000 per violation. § 503.001(d).

⁶⁵ 740 ILCS § 14/15(e) and § 503.001(c)(2),

⁶⁶ RCW § 19.375.020(4)(a).

⁶⁷ Cal. Civ. Code § 1798.150.

protect the security, confidentiality, and integrity of private information, including its disposal. N.Y. Gen. Bus. Law § 899-bb(2)(a). Under the law, covered entities have reasonable safeguards either where they (1) are a compliant regulated entity under HIPAA, GLBA, or NY DFS Cybersecurity Regulations, or (2) implement a data security program that includes a number of enumerated administrative, technical, and physical safeguards and timely dispose of personal information after it is no longer needed.⁶⁸

The HIPAA Security Rule, which regulates biometrics in certain contexts, also takes a more specific approach to outlining data security requirements, though it is designed to be flexible and scalable given the diversity of the healthcare marketplace.

Given the permanent nature of biometrics and potential security risks, a relevant question for evaluating proposed legislative frameworks is whether establishing a baseline standard is advisable or whether something more should be imposed, for example a risk analysis and management requirement, as well as technical, administrative, and physical safeguards for the information. Although specific requirements are less flexible, they lead to more certainty for businesses when designing their compliance programs and defending against enforcement actions. However, technological advances advocate for flexibility in application to prevent potential multiple applications of older statutes designed specifically for outdated technologies, which also leads to less clarity.

Consideration should also be given as to whether documented adherence to a recognized data security standard could constitute an affirmative defense to a tort or statutory claim. While this is typically the practical effect of having a data security program that aligns with established standards, this could be established as a safe harbor to liability, similar to the approach taken in Ohio.⁶⁹

C. Biometric Surveillance Laws

A small but growing number of U.S. municipalities and counties have introduced legislation regulating biometric applications.⁷⁰ In many cases that effort consists of banning or severely restricting, the use of surveillance technologies that include biometric applications.⁷¹ Currently, most of those laws apply to law enforcement and other public entities. But some local

⁶⁸ N.Y. Gen. Bus. Law § 899-bb(2)(b).

⁶⁹ Ohio Rev. Code § 1354.01, et seq.

⁷⁰ See, e.g., S.F. Admin. Code, §§ 19B.1 to 19B.10; Boston, Mass., Municipal Code, ch. XVI, § 16-62; Springfield, Mass., Code, ch. 173, § 173-1 et seq.; Berkeley, Cal., Municipal Code, ch. 2.99, § 2.99.010 et seq.; Oakland, Cal., Code of Ordinances, ch. 9.64, § 9.64.010 et seq.; Oakland, Cal., Code of Ordinances, ch. 9.64, § 9.64.010 et seq.; Cambridge, Mass., Code of Ordinances, ch. 2.128, § 2.128.075; Portland, Me., Code of Ordinances, ch. 17, § 17-129 et seq.; Minneapolis, Minn., Code of Ordinances, ch. 41, § 41.100 et seq.; King County, Wash., Code, ch. 2.67, § 2.67.010 et seq.

⁷¹ A more in-depth discussion of the use of surveillance technology may be found in Sedona's companion publication *Commentary on Notice and Consent Principles for Facial Recognition Technology*.

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to comments@sedonaconference.org no later than May 27, 2022.

governments, such as Portland, Oregon and Baltimore, Maryland, have taken the extra step to ban private-sector use of facial-recognition technology, as well.⁷²

At the state level, Maine has enacted a ban on the use of facial-recognition technology by schools, government employees, and law enforcement,⁷³ and Virginia law prohibits law enforcement from purchasing facial-recognition technology unless expressly authorized by statute.⁷⁴

Finally, enactment of biometric-privacy laws requiring disclosure of the collection and use of biometric information (as defined by the relevant law) has also begun at the local level. In 2021, New York City passed a law with similarities to Illinois BIPA. That law requires covered businesses to provide notice of the “collection, retention, conversion, storage or sharing,” of “biometric identifier information” and that prohibits profiting from the transfer of biometric identifier information. The law also provides for a private right of action for statutory damages for individuals aggrieved by a violation of the law.⁷⁵

⁷² See, Portland, Oreg., City Code, tit. 34, §§ 34.10.010 et seq.; Baltimore City Code Art. 5 § 41-4 (ban on public use), Art. 19 § 18-1 (ban on private use).

⁷³ 25 M.R.S. § 6001.

⁷⁴ Va. Code Ann. § 15.2-1723.2.

⁷⁵ NYC Administrative Code §§ 22-1201 to 22-1205