

The Sedona Conference Draft Biometric Privacy Primer (October 2021)



This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission.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 November 29, 2021.

The Sedona Conference Draft Biometric Privacy Primer (October 2021)

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)

This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission.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 November 29, 2021.

Prefatory Note for WG11 Midyear Meeting

This draft represents a work in progress with some sections relatively more developed and others, especially Part IV, relatively less developed from the original Brainstorming Group Outline. Given the diverse views represented in the Drafting Group and the sometimes sharp differences over how to approach (or even characterize) some of the issues this Draft presents, we want to emphasize that we have not yet reached complete consensus in the presentation of many important issues discussed in the current version.

Issues for WG11 Midyear Meeting Discussion

We are primarily interested in receiving feedback from the full WG11 community regarding: (1) the overall approach the current draft has taken to presenting this material, including our proposed audience(s); (2) whether we are missing key information that should be included; and (3) suggestions to refine the material, including ideas for including practical advice.

We also are interested in feedback on several specific additions/changes we are considering, including:

1. Include a Glossary of Technical Terms?
2. Develop Biometric System Selection/Deployment Considerations/Guidelines? (*See, e.g., [Commentary on Ephemeral Messaging](#)*).
3. Convert Legal Summary into a chart and focus on differences in approach/specific issues (which ones?).
4. Add Biometric Use Cases/Benefits?

I. INTRODUCTION

This Primer is intended to provide 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 I below, the Primer focuses primarily on the use of biometric identity verification and identification systems by private organizations. We focus on verification and identification systems because biometric information is most often used in these applications. 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

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 November 29, 2021.

and policy aspects of biometric systems with a particular focus on the privacy and related concerns these systems often are charged with raising.

[expand with specifics, including the idea of adding guidelines per below]

II. OVERVIEW AND EXAMPLES OF BIOMETRIC 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. Internet of Things (IoT) and edge computing devices as well as smart phones increasingly incorporate biometrics, and advances in artificial intelligence (AI), including neural networks, will continue to contribute to widespread adoption of biometrics.

The growth of biometric technology is due, in part, to the presumption that biometrics offer a more secure, faster, cheaper, simpler, frictionless, and more user-friendly alternative than other forms of information security, such as passwords and physical tokens. This presumption is based on the idea that biometric security relies on unique, persistent physical features that a person must physically present to gain access. Critics of biometric security note that many biometric features, such as a person's face, gait, and even fingerprints are difficult or impossible to keep private as they are visible to the public-i.e. everyone can see an individual's face, see how s/he walk and leave fingerprints with whatever s/he touches. Proponents of biometrics point out that biometric systems rely on proprietary templates that cannot easily be replicated even with access to a publicly available feature, like a person's face.

The rapid growth of and innovations in biometric technology prompted questions and concerns from some corners about how collection and use of biometrics may impact a person's privacy, security, and civil liberties. For example, a person's biometric characteristics are not easily changed or altered, and some private companies and governments are able to collect certain forms of biometric data with relative ease and without consent. Other questions can arise as to what disclosures the collecting entity provides as to its use of biometric information it collects, how and for how long the information will be maintained, and whether it will be shared.

A minority of state and municipal 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 municipalities have banned governmental and police use of facial recognition technology, a few cities prohibit any use of facial recognition technology, more

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 November 29, 2021.

states have taken up biometric privacy legislation, and industry groups are increasingly advocating for best practices guidelines and other forms of self-regulation.¹

B. Lack of Definitional Clarity

The term “biometrics” can be used to describe an array of technologies and processes in differing domains, and the lack of precision behind the intended meaning of the term can create confusion. For example, biometrics describes a branch of biology that uses statistical models to analyze quantitative biological observations. On the other hand, various data privacy laws have differing statutory definitions for what constitutes biometric technology. In common usage, however, biometrics is frequently used as a short-hand form of “biometric authentication” or “biometric identification.”

For purposes of this technical overview we use the following practical definition to describe the identification and authentication biometric applications that are most often cited as raising the privacy and related concerns this Primer discusses: *the measurement of a biological feature of a person, expressed in electronic form, used in software applications.*

C. Biometric Authentication and Identification Systems Overview

Biometric systems serve a variety of functions, but the most widespread applications generally are designed to either authenticate or identify an individual using one or more physical and/or behavioral characteristics:²

Authentication, or 1:1 matching: authentication occurs when a person (such as a user of a computer system) begins by claiming a specific known identity, and submits information to be used to verify that claim by comparing that information to some previously stored or enrolled information for that person. The software only compares the submitted information and the stored information. Authentication compares an existing template of the biometric identifier to a newly acquired 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.

Identification, or 1:n matching: identification systems compare a newly acquired biometric template to a database of stored templates in order to identify an unknown person. Sometimes identification is used to streamline access to systems, allowing one touch access to electronic medical records and pharmaceutical cabinets in healthcare. Another use of identification search is to prevent and detect alias or duplicate enrollments, whether accidental or intentional, called

¹ cites

² Other types of biometric data are collected in other contexts, such as certain types of health and genetic information. This Primer generally focuses on the collection of biometric information through identification and verification systems.

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 November 29, 2021.

“scrubbing” for double identity holders. Identification is also used by law enforcement and for background checks to search for matches against FBI criminal databases as part of character and fitness for bar membership, fiduciary licensure, and to check volunteers who will work with children under the PROTECT ACT, among others. Law enforcement facial recognition systems employ 1:n (and n:n) matching in public spaces to assist in identifying potential criminal suspects.³ Private commercial entities have similarly used facial recognition systems to identify individuals accused of prior shoplifting and premium customers.⁴

With respect to both authentication and identification, because software applications require inputs to be in the form of electronic data, implementing an electronic identification and authentication system means defining an identity as a mathematical representation. In such a system, the identifying information must be in a format that can be accepted as or converted to a stream of digital bits. The system then compares this digital identifier to a single credential (1:1) or a collection of authorized credentials (1:n) to find a match. Authentication systems grant the user access to the resources permitted for that identity and may log the ensuing activity with that identity. Identification systems typically confirm an identity match and/or provide a list of potentially matching identities.

In traditional knowledge or possession-based identification and authentication systems, the authorized credential takes the form of a shared secret such as a password or a private certificate key, or a physical token such as an encrypted dongle that generates a one-time key. Such systems are vulnerable to users forgetting, misremembering, or sharing their passwords, or physically misplacing or losing the token device. In other words, disclosure of a subject’s stored credential compromises their account’s security.

In contrast, biometric systems rely on measuring, storing, and comparing measurements derived from a person. The most prevalent biological characteristics that are suited for biometric system usage are those that are:

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;

³ 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.

⁴ 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>.

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 November 29, 2021.

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

Acceptable: individuals do not generally object to having it measured or scanned.⁵

As a consequence of these requirements, only biological characteristics that cannot easily be changed are useful for authentication and identification. Furthermore, some biological features, like a person's face, often are publicly available. Both of these aspects contribute to the privacy and security concerns often associated with biometric systems, including the potential risk 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. However, many systems are proprietary and not interoperable and, thus, the biometric information cannot be used across systems.

Proponents of biometric-based authentication have argued that it effectively ties the identification process to the subject him or herself, as opposed to a secondary attribute like the subject's password or token. In many implementations, this can mean that for a subject to pass a biometric authentication, that person must be physically present. Unlike passwords or tokens, the biological features used to generate biometric data cannot be forgotten, misremembered, shared, guessed, or borrowed.

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 principles⁶:

Security: It should be computationally infeasible to reverse a protected template back to the original biometric characteristic;

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.

⁵ Wayman, Jain, Maltoni, and Maio (Eds), *Biometric Systems: technology, Design and Performance Evaluation* (Springer, 2005), pp. 3-4.

⁶ Jain, Ross, and Nadakumar, *Introduction to Biometrics* (Springer, 2011), pp. 286-287.

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 November 29, 2021.

For privacy and security reasons, the amount of information contained in a template should be limited to the minimum necessary to identify matches, without revealing data that would allow an attacker to replicate the original biometric trait. One basic measure of the accuracy of a biometric system is the rate of false matches (AKA Type 1 Errors, or False Positives) and the rate of false non-matches (AKA Type 2 Errors, or False Negatives). Generally speaking, improving the accuracy with respect to a Type 1 Error will degrade the accuracy with respect to a Type 2 Error, and vice versa. The desired balance of Type 1 versus Type 2 accuracy will vary depending on the specific use case involved.

D. Biometric Authentication System Technical Basics

Most biometric systems follow a basic operating model that includes the following components:⁷

Acquisition and Enrollment: software captures a raw data sample of a particular physical feature from an individual. Some biometrics, like fingerprints, typically require direct contact with a device, capturing 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.

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 This description is adapted from Andrew Rice and Isabelle Moeller eds., *United Nations Compendium of Recommended Practices For the Responsible Use & Sharing of Biometrics in Counter Terrorism Final Draft* (June 2018) at 10-11, available at https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf.

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 November 29, 2021.

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.

E. 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 identification 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 minutia 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 minutia points by their orientation and coordinates on an x/y plane.⁸ 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

⁸ 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).

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 November 29, 2021.

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.

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, “Facial Geometry” is a feature-based approach that begins with measurements of specific facial features (eyes, nose, mouth, etc.) and their relationship to one another on a given face.

By contrast, Category 2 technologies use software to detect a prominent orienting facial landmark (typically, the centers of the eyes). Once the orienting landmark 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.

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 November 29, 2021.

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.⁹

Voice Recognition¹⁰

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

⁹ The concept of "Hamming Distance" is 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.

¹⁰ As discussed in Part IV, BIPA, the Texas and Washington statutes each use the term "voiceprint" which is different than voice recognition. The difference between the two and it is the subject of some litigation. [add cites]

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 November 29, 2021.

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 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.

E. Emerging Issues in Biometrics

The last few years have seen major advances in biometric technology, as developers continue to modify existing technology and develop new ways to verify and/or identify individuals based on biological, physical, and behavioral characteristics. Behavioral biometrics use a unique profile of a distinctive behavior or even a combination of behaviors ranging from how a person holds a device, swipes a screen or types on a keyboard to build a user profile for authenticating their identity.¹¹ These patterns often are combined with other information such as a person's IP address and/or location to identify suspicious authentication attempts, which the system either blocks or triggers an additional authentication method.

The rise of liveness detection, passive authentication, and dual authentication using both biometric information and behavioral characteristics, are examples of developments in biometric technology that were not anticipated at the time the first of the existing biometric statutes was enacted more than a decade ago.

¹¹ See IBIA, *Behavioral Biometrics* (date), available at <https://www.ibia.org/download/datasets/3839/Behavioral>.

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 November 29, 2021.

Issues include:

- Are these “biometrics”?
- Data Aggregation
- Immutability
- Reliability

III. Biometric Legal and Policy Issues

A. Privacy

As advocates for the use and development of biometric technology emphasize, the application of biometric technology 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.

The collection, use, and distribution of biometric information also raises a certain privacy considerations. Most fundamentally, biometrics relating to physical characteristics, such as fingerprints, palm prints, retina or iris scans, facial features, and the like, are generally immutable. These characteristics are also unique to each individual and, therefore, carry a reliable and persistent link between the individual and the individual’s characteristics. Biometric information is, in this sense, personal and constitutive.

Its unauthorized or unknown collection or use, under certain circumstances, can be viewed as an intrusion into one’s personal space and a challenge to the autonomous control of personal information.

The privacy considerations of biometrics include the following:

Individual Identification – Biometrics, particularly biometrics relating to physiological or biological characteristics, such as fingerprints, palm prints, retina or iris scans, facial features, and the like, are generally immutable and unique to each individual. These characteristics carry a reliable and persistent link to the individual and can be used for identification. This includes identity tracking.

Collection Without Knowledge – Certain biometric information can be collected without the knowledge of the individual. For example, facial recognition or voiceprint technology can be utilized without the individual being aware. And even other modalities which generally require direct interaction with the collection device (e.g., fingerprint placed onto a finger scanning device), may allow for capture through indirect means (e.g., lifting a fingerprint from an item touched by the individual) that allows for the covert collection of information.

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 November 29, 2021.

Collection Without Required Form of Consent – Biometric information privacy statutes or regulations may mandate that consent be obtained in a particular manner, such as requiring written consent prior to collection. In circumstances in which an individual is aware their biometric information is being or may be collected, such form of consent may nevertheless implicate the individual's privacy interests in, for example, the use, retention or safeguarding of biometric information.

Individual Information Aggregation – The use of biometrics to identify an individual can be aggregated or combined with other sources of personal information to form a more detailed profile of the individual. This can involve attaching certain additional information about an individual, such as political or religious affiliation, as part of the aggregated individual information.

Secondary Information – Biometric information may contain secondary information that can be harvested and used beyond the individual's knowledge or consent. For example, retina or facial biometric information may contain secondary information relating to the individual's health. And an individual's DNA is perhaps the most extreme example of the potential to gather secondary information from biometric information.

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 identified surreptitiously – most notably, facial recognition technologies.

Expansion of Use – Even if biometric information is collected or obtained with the knowledge and consent of the individual, the use or application of that biometric information beyond the function for which the individual understood it was collected implicates privacy considerations.

B. Security and Integrity

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

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 November 29, 2021.

one system, it cannot be used to reverse engineer the biometric attributes of templates from another system.

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 dissimilar two system algorithms are the same, then exfiltration of the 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 (authentication, or 1:1 matching, vs identification, or 1:n matching).

C. Function Creep

Function creep is what happens when technology, data, or information is used beyond its originally stated purpose.

A classic non-tech example is the United States' Social Security number (SSN). SSNs, first issued in 1936, were originally intended only to track earnings to determine social security benefits.¹² “Not for identification” was printed on each card.¹³ By the 1960s, however, the IRS

¹² <https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html>

¹³ <https://www.ssa.gov/history/ssn/ssnversions.html>

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 November 29, 2021.

began using SSNs for tax identification purposes.¹⁴ In the following decades, the SSN became a ubiquitous personal identifier for governmental, commercial, and consumer purposes. SSNs are required for access to federal benefits like Medicare, veteran's affairs services, and food assistance; the opening of savings accounts or receipt of loans; work authorization; establishing and obtaining credit; and credit-related authorizations required to access services ranging from public utilities to insurance to cell phone plans, *inter alia*.

Along with that widespread utility arose motives for misuse. With SSNs a barrier to entry for so many vital services, SSN theft can give someone much-needed access to services or work for which they may not otherwise qualify. SSN thieves can buy goods, enroll in services, or obtain credit with someone else's SSN, avoiding the consequences of nonpayment. Bad actors can access or steal unique benefits earmarked for the actual SSN holder. And with so many crucial data points associated with SSNs, a SSN can be misused beyond identity theft to obtain data and information about an individual for any number of purposes.

That said, while SSNs are intended to be permanent, lifelong numbers – they can be changed when the need arises.¹⁵ Biometrics, however, are different in that regard. They are largely permanent and immutable. Because of this distinction, lessons learned from other “personal identifier” contexts must be considered and applied with great care in evaluating the impact of function creep in connection with biometric-related technologies.

In the biometric context, function creep may occur for any number of reasons. It can be born out of innovation or need. 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 brushfires and provide them aid.¹⁶ During the Covid-19 pandemic, biometric technology has been used to scan for health metrics like fever,¹⁷ to develop technology that could allow public health officials to identify individuals who are not obeying stay-at-home

¹⁴ <https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html>

¹⁵ <https://www.consumer.ftc.gov/articles/0248-do-you-need-new-social-security-number>

¹⁶ <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>

¹⁷ *E.g.*, <https://academic.oup.com/jlb/article/7/1/Isaa038/5857112>

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 November 29, 2021.

orders or mask mandates,¹⁸ or to provide touchless admission to large events (while also assessing temperature and mask use)¹⁹.

Function creep may also occur as the use of biometric data evolves to meet a commercial purpose. For example, a company might implement employee facial recognition for building access, and later using it to monitor employees' arrival and departure times and whereabouts in a building. Function creep can be profit-motivated – like a company's collection of biometric data for a consensual, consumer purpose, and its subsequent sale of that information for profit. Or it may be nefarious, involving the criminal misuse or theft of biometric data, or the surreptitious transfer of data to countries lacking strong privacy protections²⁰. Even function creep that arises with good intentions may lead to problematic consequences – like expanding governmental biometric use to private contexts in a way that creates barriers for individuals' access to good or services²¹.

Regardless of its purpose, function creep invariably implicates a number of privacy considerations. The use of biometric data requires a balancing of security, privacy, and necessity – new uses may shift, or entirely upend, that balance. Perhaps the most fundamental concern is consent. Function creep raises questions about whether the original source of the biometric data provided informed consent to the new use scenario. Function creep can also impact security; using biometric data for new purposes often means increased access, storage points, and potentially disclosure of that data. Likewise, the quality and integrity of biometric data require examination when function creep arises. The integrity of biometric data may be suitable for one purpose (e.g., home security) but not for a new purpose (e.g., criminal identification by law enforcement).

One of the most often-raised data privacy risks in any context is that of aggregation, which is itself a form a function creep – e.g., the risk that information from multiple sources can be combined to create a dossier of an individual's habits, preferences, actions, statements, movements, appearance, and personal and familial connections. If this information were linked by a name, a credit card number, or an IP address, for example, the link between the data points

¹⁸ See, e.g., <https://www.forbes.com/sites/zakdoffman/2020/03/05/meet-the-coronavirus-spy-drones-that-make-sure-you-stay-home/?sh=44fab36f1669>; <https://theconversation.com/coronavirus-drones-used-to-enforce-lockdown-pose-a-real-threat-to-our-civil-liberties-138058> [NOTE that these links are about capabilities, not implementation, of facial recognition w/ drones]

¹⁹ <https://www.axios.com/sports-facial-recognition-coronavirus-4b84d170-8455-4949-8953-8f56b8855ee3.html>

²⁰ See, e.g., <https://time.com/6071773/tiktok-faceprints-voiceprints-privacy/>; <https://www.forbes.com/sites/zakdoffman/2019/05/20/u-s-government-warns-chinese-made-drones-may-be-secretly-sharing-data-with-china/?sh=65f143992d27> [concerns re possible data transfer to china]

²¹ E.g., <https://time.com/5409604/india-aadhaar-supreme-court/> (noting lack of proof of identity required to sign up for biometrics service; health issues that may make an individual unable to provide a fingerprint or eye scan).

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 November 29, 2021.

(and future aggregation) could theoretically be broken by changing some of these identifiers. But because biometric data is immutable, data aggregation cannot be undone or stopped in the same way. If function creep arises in association with biometric data, information about an individual could grow and aggregate exponentially and permanently.

Indeed, 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. This combination creates the real prospect that private companies and law enforcement agencies will be able to combine more and better biometric data and other information in ways that compromise individual privacy to a far greater extent than any single application.²² These new capabilities both intensify the privacy risks posed by these technologies and complicate the challenge of developing laws and policies that address the issues posed by potential aggregation and redeployment of individual biometric information.

The public nature of some biometric features opens the door to collection and use of information, like photographs and voice recordings, that can easily be converted for use in biometric applications without disclosure or consent of the individual. Indeed, the profusion of privately uploaded images and voice recordings tagged with individual names on social media and other internet platforms and their use by private companies to train biometric systems algorithms is credited as one of the drivers in dramatic improvements in facial recognition technology while raising concerns over whether and how access to those images should be regulated.²³

Even where user consent is obtained before collecting facial images and voice recordings, that information easily can be redeployed and processed by biometric systems for very different purposes. The potential for private biometric systems to share information with law enforcement and national security agencies intensifies these concerns. In 2015, the FBI quietly announced that it would start to retain fingerprints submitted for routine background checks in its searchable criminal database.²⁴ In 2018, Interpol completed a pilot of the largest law enforcement voice recognition system that uses recordings from social media sites, among other sources.²⁵

²² AI Now, *Regulating Biometrics: Global Approaches and Urgent Questions* (2020), at 7-8.

²³ Cite Clearview AI

²⁴ <https://www.eff.org/deeplinks/2015/09/little-fanfare-fbi-ramps-biometrics-programs-yet-again-part-1>

²⁵ Interpol's New Software Will Recognize Criminals by Their Voices <https://spectrum.ieee.org/interpol-s-new-automated-platform-will-recognize-criminals-by-their-voice>; see also <https://vimeo.com/219362794> (promotional video explaining that the system searches suspect recordings against social media sites for potential matches).

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 November 29, 2021.

Internationally, there are reports²⁶ of government-obtained biometric data being linked with DNA.²⁷ Likewise, many U.S. states have included face templates derived from driver license photographs in their facial recognition databases, often without any specific legal authorization or notice to the public.²⁸ Some state and federal agencies also pay to access private facial recognition databases where the consent questions are even murkier.²⁹

Recent U.S. House and Senate investigations into law enforcement access to private biometric databases have highlighted the often blurred lines between private and public use of biometric information and even prompted legislation.³⁰ One facial recognition company obtained close to three billion face images with names attached by scraping public web sources without consent from the individuals. The company marketed facial recognition surveillance tools to both private and public entities claiming that its system could identify persons of interest and connect them to other intimate information. This and related examples demonstrate the ease with which private biometric information can be obtained and shared with law enforcement with relatively little scrutiny or regulatory oversight.³¹

These examples also illustrate a related set of concerns: law enforcement increasingly relies on private companies to collect, process and store sensitive biometric information. [expand].

²⁶ *E.g.*, <https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions>; **ADD CITEs/alternative sources**

²⁷ Relatedly, advances are being made to reverse-engineer individuals' appearances (and perhaps, one day, biometrics) from DNA. *E.g.*, <https://www.popsi.com/new-service-reverse-engineers-faces-dna-samples-crime-scenes/>; <https://www.nytimes.com/2017/10/19/nyregion/dna-phenotyping-new-york-police.html>; **ADD CITE re reverse-engineering faces**

²⁸ Cite Georgetown study.

²⁹ See Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," The New York Times (Jan. 18, 2020), at <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

³⁰ 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]

³¹ See, *e.g.*, Sen. Ed Markey, "Senator Markey Investigation into Amazon Ring Doorbell Reveals Eggregiously 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-eggregiously-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).

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 November 29, 2021.

D. System Accuracy

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).³²

Accuracy is a relative concept that can vary 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 how its ability to correctly identify a single individual across multiple different photos.³³ Accuracy also depends on how a system is configured and actually used in real life. The following list identifies and briefly describes the most significant factors that can affect the accuracy of biometric systems:

Image Quality: the quality of used to create the biometric template at the enrollment phase and of the probe image used to verify or identify a person severely affects the accuracy of the system.³⁴

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 also is heavily influenced by the quality, quantity and diversity of the data used to train the system. Accuracy also often varies significantly across different demographic groups.

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

³² Patrick Grother, et al., *Facial Recognition Vendor Test (FRVT): Part 2: Identification*, NISTIR 8271 Draft Supplement (2020), 2-3.

³³ See Stephen Fontenot, “Study Outlines What Creates Racial Bias in Facial Recognition Technology,” Univ. of Texas at Dallas News, Dec. 4, 2020, available at <https://news.utdallas.edu/science-technology/racial-bias-facial-recognition-2020/>

³⁴ *Id.* at 4-5.

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 November 29, 2021.

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.³⁵

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.

These factors operate together to determine the accuracy of a given biometric system. The recent misidentification of Robert Williams as a suspect in a robbery by Detroit police using the Michigan State facial recognition system illustrates this interactivity. According to media stories, the Detroit police used a low-resolution screen capture from a surveillance camera as the probe photo and the search returned Mr. Williams' photo as a potential match.³⁶ Michigan uses a system that has scored highly on the NIST FRVT tests, but those scores are based on relatively high-quality photographs.³⁷

E. Discrimination, Bias and Fairness

Biometric systems and algorithm-based decision systems more generally frequently are charged with operating directly to discriminate against certain groups and/or as being used to perpetuate and exacerbate existing discriminatory structures or processes. 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.³⁸

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).³⁹ From a technical performance perspective, it is relatively straightforward to measure and quantify how a system performs on a specific metric across different

³⁵ See Jacqueline G. Cavazos, et al., *Accuracy Comparison Across Face Recognition Algorithms: Where Are We on Measuring Race Bias?*, 3 IEEE Transactions on Biometrics, Behavior, and Identity Science 101 (2021).

³⁶ Bobby Allyn, “‘The Computer Got It Wrong:’ How Facial Recognition Led to False Arrest of Black Man,” NPR, June 24, 2020, available at <https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig>.

³⁷ Paresh Dave, “Face Recognition vendor vows new rules after wrongful arrest in U.S. using its technology,” Reuters, June 24, 2020, available at <https://www.reuters.com/article/us-michigan-facial-recognition/u-s-activists-fault-face-recognition-in-wrongful-arrest-for-first-time-idUSKBN23V1KJ>; <https://www.rankone.io/> (citing NIST FRVT results).

³⁸ 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>.

³⁹ *Id.* at 3.

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 November 29, 2021.

demographics.⁴⁰ For example, a 2019 study by NIST concluded that most of the facial recognition algorithms it tested in the FRVT program, with some notable exceptions, had higher error rates for some demographic groups for both verification (1:1 matching) and identification (1:n matching).⁴¹

But demographic differences can affect system performance in multiple ways. Thus, one study demonstrated that even where different facial recognition algorithms produced similar results for high-quality images of East Asian and Caucasian faces, the accuracy dropped far more for East Asian faces in low-quality images than it did for low-quality Caucasian images.⁴²

Even where a biometric system meets a set of technical standards for accuracy and non-bias in a test setting, it may well 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.

The risk of discrimination is exacerbated by the frequent lack of transparency in the deployment of these systems and the widespread use of privately created “watch list” databases.⁴³ Individuals often have no way of knowing that a private system has flagged their biometric information (most often facial templates created from surveillance camera footage) or any opportunity to contest it.⁴⁴ 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.⁴⁵

The relative over-deployment of biometric systems in communities of color as well as the overrepresentation of racial minorities in law enforcement facial recognition databases raise related problems of bias and fairness that cannot be addressed by improving system performance.

⁴⁰ *Id.*

⁴¹ <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>.

⁴² See Cavazos, *supra* n. __ at 108.

⁴³ 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).

⁴⁴ 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>

⁴⁵ 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-c13fff8d-72c6-400f-b680-6ae2679955d4.html>.

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 November 29, 2021.

The rapid evolution of biometric systems promises eventually to make these systems highly accurate across all demographics. While this would resolve one set of concerns over exclusion and misidentification, the disparities in deployment of these systems means that these communities may disproportionately be affected by loss of privacy and diminishment of civil liberties posed by the potential for mass surveillance that expansive deployment of these systems poses.

G. Transparency and Explainability

A related set of concerns arise from the use of advanced technologies like deep neural networks and other advanced machine learning techniques in biometric systems. These new methods improve the speed, accuracy, precision, and scalability of biometric systems. At the same time, however, their increasing complexity makes it difficult for even experts to adequately explain what variables influence the decisions these systems make. Transparency and explainability are necessary for meaningful oversight and accountability as well as to uncover potentially hidden forms of bias.

IV. EXISTING LAWS AND PRINCIPLES

A. Overview

As noted above, there are a growing number of federal and state legislative proposals to regulate the use of biometric systems directly or as part of a broader data privacy and security bill. And there are frequent proposals to amend existing laws, including BIPA. Eleven states – Arkansas, California, Colorado, Illinois, Maryland, New York, Oregon, Texas, Virginia, and Washington – have enacted statutes that regulate biometric privacy, with five statutes specifically addressing it. Twenty-two states (including some with regulations in place) have additional proposed legislation pending; eleven of those are focused specifically on biometric data collection any privacy. Biometric information is separately regulated by some other states' consumer privacy statutes, including the California's consumer privacy law. Many states have also amended their data protection and breach notification laws to include biometric information.

At the federal level, the Federal Trade Commission's general consumer protection authority over data privacy and security encompasses biometric information and sector-specific laws like HIPAA also regulate some biometric information and/or practices related to that information.

Government acquisition and use of biometric information is governed broadly by the U.S. Constitution 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 proposed regulations have been successfully challenged by privacy organizations.⁴⁶

⁴⁶ <https://www.eff.org/deeplinks/2021/06/victory-biden-administration-rescinds-dangerous-proposed-rule-expand-biometrics>

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 November 29, 2021.

Beyond these, a number industry groups, governmental entities and privacy organizations have published guidelines and standards.⁴⁷

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. The discussion of specific existing laws below attempts to focus on a set of general issues that most of these laws address with a specific focus on the Illinois law because it has been litigated far more than other laws and thus offers the best opportunity for analysis of the challenges that arise in regulating this area.

B. Legislative Trends and Issues

[Expand and pull relevant issues from sections below]

- Current laws apply broadly to most private entities but exclude public entities.
- Some critics of these laws have called for narrowing their scope and a number of amendments to BIPA were proposed, none of which have yet been passed. These proposed amendments were largely directed to issues that have surfaced in the litigation including, but not limited to limiting the scope to exclude biometric data collected in the employment context, proposing a statute of limitations, limiting and/or clarifying damages, including a cure period, clarifying consent as well as other proposed revisions.
- Conversely, others have criticized the exclusion of public entities due to the ease with which government entities can obtain privately collected biometric data, and the difficulty in clearly demarcating public and private activities.
- A related issue is whether biometric information should be regulated under a separate statute or incorporated into existing comprehensive consumer privacy laws. The California law is an example of an integrated approach.

C. U.S. Consumer Biometric Privacy Laws

1. Biometric/Covered Information Definition

The rapidly evolving nature of biometric technology and the challenges defining the term “biometric” have led to significant legal disputes concerning the definition of biometric information. Definitions under operative and pending state statutes vary, and litigation has centered on some such questions. For example, the Illinois statute defines biometric information generally, specifically includes a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry), and expressly excludes certain data elements from the definition of “biometric identifier” (such writing samples, photographs, tattoo descriptions, information captured in a health care setting or under HIPAA).

⁴⁷ See e.g., <https://www.nist.gov/programs-projects/biometrics>; Oakland Privacy Commission Proposal on Regulation; Others?

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 November 29, 2021.

How to apply the definition to newer technologies and the scope of the exceptions has been the subject of debate, especially photographs and whether facial recognition technology is covered under BIPA.⁴⁸ New challenges to voice collection, for example, are a recent cutting-edge topic.

California's law uses a different model. It 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. 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

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. Many laws also tend to make exceptions for uses that are pursuant to a valid warrant or subpoena.⁴⁹

3. No Sale/Disclosure

Current and proposed laws address sale and disclosure of biometric data by prohibiting the sale or profit from biometrics and/or placing restrictions on their disclosure. For example, BIPA prohibits "private entity[s] in possession of a biometric identifier or biometric

⁴⁸ To date, this issue has only been addressed on the merits in the [cite Facebook].

⁴⁹ For example, BIPA exempts financial institutions or affiliates subject to GLBA; information captured from patients in a health care setting; HIPAA covered information; or information collected, used, or stored for health care treatment, payment, or operations; and exempts State or local government agencies, any court of Illinois, a clerk of the court, or a judge or justice thereof; and contractors or agents working for the state or local government. 740 ILCS 14/10, 14/25(b), (c). That law also clarifies that it should not be construed to impact the admission of biometrics in court or other proceedings. *Id.* at 14/25(a). 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."

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 November 29, 2021.

information” from selling, leasing trading “otherwise profit[ing]” from a person’s biometric identifiers or biometric information.⁵⁰ The scope and application of this provision is unclear. For example, some have argued that a private entity that sells a “biometric device” or hosts such data for a fee are “otherwise profiting” from a person’s biometrics. Such broad arguments, if successful, could substantially curtail or eliminate the ability of companies providing biometric technology or data hosting from operating in the State.

By contrast, California’s law includes biometrics as part of personal information. That statute permits businesses to sell personal information (with “sell” being broadly defined to include any transfer or disclosure for value), but they must provide individuals with a right to opt out.⁵¹

Consumer biometric privacy laws also place restrictions more generally on the disclosure of biometrics, permitting disclosure only where there is notice and consent; where the disclosure is necessary to provide a product or service explicitly requested by the individual (Washington); or to effectuate a financial transaction (BIPA).⁵² Allowances are also made for where the disclosure is required by law or made pursuant to a warrant or subpoena.⁵³

Issues often raised with respect to disclosure restrictions include: whether anyone should benefit from the sale of biometric disclosures, especially when disclosure of how such information is collected and used may be less than understandable to the average person; the right to refuse collection, the issue of notice/informed consent before disclosure or a right to opt out, potentially afterwards, with the attendant questions of whether biometric disclosures, or the related consent, can be rescinded effectively. In addition, there is also the question of whether it makes sense to write service-provider exceptions into a law, and under what circumstances, and whether individuals can sell or profit off of their own biometric disclosures.

There are also consent-related concerns with disclosures to third parties, including ensuring that the scope of the original notice/consent covers the intended use(s) by third parties, as discussed in further detail below.

5. Notice/Consent

⁵⁰ 740 ILCS 14/15(c).

⁵¹ Cite. Other laws regulating the use of biometrics also require consent prior to disclosure. For example, FERPA, which regulates “biometric records” as “personally identifiable information,” generally requires consent prior to the disclosure of personally identifiable information in student records to third parties, subject to certain exceptions. 34 CFR §§ 99.30, 99.31.

⁵² cites

⁵³ Cite.

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 November 29, 2021.

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.⁵⁴

For example, BIPA requires written notice that biometrics are being collected and the “specific purpose and length of term” for the collection/use/storage, and the entity collecting the biometrics must obtain a written release prior to their collection or receipt.⁵⁵

California’s law permits businesses to sell personal information, including biometric information, but requires notice and a right to opt out. 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 stop a business from distributing the data within the organization that collected it (even to different business units). Businesses who 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.⁵⁶ There are some timing questions about how the notice and opt-out provisions apply and whether there may be a gap between when an individual requests an opt-out and when the business ceases selling the information.

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.⁵⁷ 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.⁵⁸ 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.”⁵⁹

⁵⁴ 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 (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.

⁵⁵ cite

⁵⁶ cite

⁵⁷ RCW 19.375.020(2).

⁵⁸ *Id.*

⁵⁹ *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.

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 November 29, 2021.

6. Retention

As discussed in Part III above, biometric information generally is considered personally identifiable information that poses privacy and security concerns when collected and retained. To address these concerns, some statutes clarify retention requirements. Most laws also generally impose an upper limit on the retention period, pegged to the purposes or services for which the biometrics were collected.⁶⁰ Most laws include [add Considerations] 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/Penalties

Existing biometric privacy laws 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.

BIPA provides a private right of action.⁶¹ Current Illinois caselaw allows for standing in federal court even where there is merely a statutory violation; a showing of harm is not a requirement. Whether there is standing under Illinois state law has not yet been adjudicated. 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.⁶² Other states, like Texas and Washington, restrict enforcement to their respective state attorney general.⁶³

⁶⁰ 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).

⁶¹ 740 ILCS § 14/20.

⁶² Cite.

⁶³ Wash. § 503.001(d); Tex. RCW § 19.375.030(2).

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 November 29, 2021.

There is a long-standing policy debate over the relative merits of permitting private enforcement actions for consumer rights versus limiting enforcement to a regulatory authority like a state attorneys general. [expand].

Each of the biometric privacy laws provides 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.⁶⁴ Other states provide statutory cap per violation.⁶⁵

[add discussion of debate re: calibrating penalties]

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.”⁶⁶ The Washington law requires only “reasonable care.”⁶⁷

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.”⁶⁸

The general trend in data security laws is towards 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 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

⁶⁴ Negligent violation: greater of liquidated damages of \$1,000 or actual damages. 740 ILCS 14/20(1). Intentional/reckless violation: greater of liquidated damages of \$5,000 or actual damages. 740 ILCS 14/20(2). Reasonable attorneys’ fees and costs. 740 ILCS 14/20(3).

⁶⁵ Washington Not more than \$2,000 per violation. RCW § 19.375.030(2); RCW § 19.86.140. Texas: Civil penalty of not more than \$25,000 per violation. § 503.001(d).

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

⁶⁷ RCW § 19.375.020(4)(a).

⁶⁸ 1798.150.

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 November 29, 2021.

enumerated administrative, technical, and physical safeguards and timely dispose of personal information after it is no longer needed. N.Y. Gen. Bus. Law § 899-bb(2)(b).

The HIPAA Security Rule, which also 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 sensitive, permanent nature of biometrics and potential security risks, a relevant question for evaluating proposed legislation or frameworks will be 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

D. HIPAA Privacy Rules

Protected Health Information (PHI) is any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA-covered entity. PHI also includes biometric identifiers, including fingerprints and voiceprints.⁷⁰

Covered entities (CE) include health care providers, health plans, and healthcare clearinghouses. Entities that support covered entities in carrying out their operations or managing their information must also comply with HIPAA.

Key concepts and principles under HIPAA include ensuring a federal “floor” of privacy protection rather than a “ceiling,” which preempts any state laws that do not provide the same level of privacy protection as or are inconsistent with those federal protections. State laws with more stringent protections supersede HIPAA. HIPAA carves out the need to obtain individual consent or authorization for public health activities and public purposes established under state laws that prescribe exceptions or mandatory reporting such as for health oversight, law enforcement, organ or tissue donation, research, judicial proceedings, or when necessary to avert serious threat of harm to the individual or other persons. Otherwise, HIPAA allows for the use and disclosure of such for treatment, payment, or healthcare operations without written

⁶⁹ Ohio Rev. Code § 1354.01, et seq.

⁷⁰ 45 C.F.R. 164.512.

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 November 29, 2021.

authorization as long as the CE provides written notice of their privacy practices that clearly describes among other things such uses and disclosures, their duties to and the rights of patients, and complaint procedures. Other uses and disclosures such as research, education, marketing, or fundraising may be carved out, or permitted with or without written consent and authorization. For example, research may require either an IRB waiver or written consent. Marketing requires written authorization especially if the CE receives direct or indirect reimbursement from third parties, but it does include all communications that promote health-related products or services. Fundraising may require the opportunity to opt out. An individual also has the right to access or obtain copies of their PHI and obtain an accounting of disclosures made to unauthorized third parties. There is no private cause of action allowed to an individual to sue for a violation of the federal HIPAA or any of its regulations.

E. GDPR

The most important non-U.S. privacy law by far is The General Data Protection Regulation (GDPR) of the European Union. The GDPR applies across 27 EU states and (effectively) the UK (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.) Non-EU established organizations will be subject to the GDPR, if they process personal data about EU data subjects. This makes the GDPR a “global” law.

The GDPR is a complex mechanism (the Preamble alone has 173 sections) embedded in the legal system of a unique international body, which in turn relies upon a “pooled sovereignty,” all of which sits against a background of State-sponsored “fundamental rights” (human rights).

The GDPR approaches consent in a unique manner (see below), and, in the first instance, is really all about “data protection” (not privacy). While it does assist individuals, it also affects risk management regimes and compliance issues for companies. And while the GDPR does, in some sense, “protect consumers,” the EU has a quite separate consumer protection laws in operation apart from the GDPR.

The GDPR definition of biometric data covers personal data (included as a special category) resulting from “specific technical processing.” This can have the effect of excluding raw personal data such as facial images captured on CCTV, voice recordings, or even raw fingerprints.

It should also be noted that the GDPR is probably better characterized as “a process” rather than “a checklist,” and some common law attorneys (and their clients) may find this civil law approach to law and governance less than crystal clear. Taking U.S. privacy torts as an example, the U.S. focus is more on stopping information from being shared; in contrast, the EU focus is more on “transparency of and accountability for” the sharing. Another critical point of contrast is that while the U.S. focuses on the data relationship (and how to manage it), the EU’s emphasis tends to follow the data as it moves around.

The EU scheme is not, in its essence, a notice-and-consent regime; rather, it focuses on the lawfulness of the data processing. While this may include a “consent aspect,” consent is by no means the magic formula for understanding how the system of protection works.

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 November 29, 2021.

With some exceptions, the GDPR covers both biometric and genetic data explicitly under the above scheme. Enforcement under the GDPR is (a) assisted by the Data Protection Law Enforcement Directive, or (DP LED), and (b) can be complicated by local variations in interpreting rules and exemptions.

D. Municipal and County Ordinances

A small but growing number of U.S. municipalities and counties have introduced legislation restricting the use of surveillance technologies that include biometric applications or in some cases banning the use of facial recognition technology by public entities and/or law enforcement. Advocates of these bans argue that facial recognition poses distinctive privacy risks over other information and biometric technologies and that law enforcement use typically lacks either express legal authorization or limitations.

E. Industry/Advocacy Group Principles

An increasing number of organizations, including trade groups, privacy advocacy groups and individual companies have published principles and best practices for biometric technologies, in particular for facial recognition technologies, which have come under increased scrutiny in recent years.

Most of these include some version of following general principles but with substantial variation in the details of how to implement them: (1) Transparency/Notice; (2) Meaningful Consent; (3) Data Quality; (4) Validated Accuracy; (5) Non-Discrimination; (6) Data Security; (7) Accountability; (8) Privacy by Design.

In addition to principles specific to biometric technologies, many groups have published recommendations for principles to govern the use of artificial intelligence in general, which would apply to most biometric technology systems. For example, NIST recently published for public comment the first draft of Four Principles of Explainable Artificial Intelligence (Draft NISTIR 8312), which recommends: (1) AI systems should deliver accompanying evidence or reasons for all their outputs; (2) Systems should provide explanations that are meaningful or understandable to individual users; (3) The explanation correctly reflects the system's process for generating the output; (4) The system only operates under conditions for which it was designed or when the system reaches a sufficient confidence in its output. (The idea is that if a system has insufficient confidence in its decision, it should not supply a decision to the user.)