The Sedona Conference Journal

Volume 25 2024

The Sedona Conference U.S. Biometric Systems Privacy Primer

The Sedona Conference

Recommended Citation:

The Sedona Conference, *U.S. Biometrics System Privacy Primer,* 25 SEDONA CONF. J. 163 (2024).

For this and additional publications see: https://thesedonaconference.org/publications.

THE SEDONA CONFERENCE U.S. BIOMETRIC SYSTEMS PRIVACY PRIMER

A Project of the Sedona Conference Working Group on Data Security and Privacy Liability (WG11)

Author:

The Sedona Conference

Editor-in-Chief:

Brian Ray

Contributing Editors:

Julian Ackert
Melissa Ryan Clark
Brett Doran
David Kalat
Colman D. McCarthy
Francis X. Nolan, IV
Lesley Weaver

Steering Committee Liaisons:

Starr Turner Drum
Ruth Promislow

Staff Editors:

David Lumia
Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 11. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

This publication may be cited as follows:

> The Sedona Conference, *U.S. Biometric Systems Privacy Primer*, 25 SEDONA CONF. J. 163 (2024).

PREFACE

Welcome to the May 2024 final version of The Sedona Conference *U.S. Biometric Systems Privacy Primer* ("*Primer*"), a project of The Sedona Conference Working Group 11 on Data Security and Privacy Liability (WG11). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG11 is to identify and comment on trends in data security and privacy law, in an effort to help organizations prepare for and respond to data breaches, and to assist attorneys and judicial officers in resolving questions of legal liability and damages.

The Sedona Conference acknowledges Editor-in-Chief Brian Ray for his leadership and commitment to the project. We thank contributing editors Julian Ackert, Melissa Clark, Brett Doran, David Kalat, Colman McCarthy, Frank Nolan, and Lesley Weaver for their efforts. We also thank Starr Drum and Ruth Promislow for their contributions as Steering Committee liaisons to the project, and we thank Mark Abramowitz for his contributions.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG11 who reviewed, commented on, and proposed edits to early drafts of the *Primer* that were circulated for feedback from the Working Group membership. Other members provided feedback at WG11 meetings where drafts of this *Primer* were the subject of the dialogue. The publication was also subject to a period of public comment. On behalf of The Sedona

Conference, I thank both the membership and the public for all of their contributions to the *Primer*.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG11 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, patent litigation, patent remedies and damages, and trade secrets. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
May 2024

TABLE OF CONTENTS

I. INTRODUCTION

This *U.S. Biometric Systems Privacy Primer* ("*Primer*") provides a general introduction to biometric systems and a summary of existing U.S. laws regulating the collection, use, and sharing of the biometric information these technologies collect.

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

As Part II explains, the *Primer* focuses primarily on biometric recognition systems (which include both identity verification and identification systems) by private organizations. 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."

II. OVERVIEW OF BIOMETRIC RECOGNITION SYSTEMS

A. Biometric Modalities and Purpose

The term "biometrics" is used generally to encompass biological or behavioral characteristics that are unique to a person and allow for identification and/or verification of that individual. Biometric recognition systems record a unique physical characteristic—or combination of characteristics—from an individual and compare that stored record to a later-acquired record of the same attribute, using software to determine whether the two records "match" each other within the parameters of a prescribed statistical range set by the system.

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

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

---

1. SOODAMANI RAMALINGAM ET AL., FUNDAMENTALS AND ADVANCES IN 3D FACE RECOGNITION, IN BIOMETRIC-BASED PHYSICAL AND CYBERSECURITY SYSTEMS 125–62 (Mohammad S. Obaidat et al. eds., 2019).

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

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

2. *See, e.g.*, *Biometrics*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/biometrics (last visited Feb. 2, 2024); Ann Cavoukian et al., *Privacy and Biometrics for Authentication Purposes: A Discussion of Untraceable Biometrics and Biometric Encryption*, *in* ETHICS AND POLICY OF BIOMETRICS, ICEB 2010, LECTURE NOTES IN COMPUTER SCIENCE 14 (Ajay Kumar & David Zhang eds., 2010).

advocating for best practices guidelines and other forms of self-regulation.

B. Biometric Recognition Systems Overview

The term "biometrics" is used across multiple disciplines to describe an array of technologies and processes ranging from identity or verification systems to biological processes like the statistical analysis of biological data. The lack of consensus over how to define "biometrics," and even what biological characteristics the term should encompass, is reflected in the differing legal definitions included in the data privacy and related laws discussed below in Part IV.

For purposes of this *Primer*, we focus on a set of technologies related to identifying individuals that fit the International Standards Organization's (ISO) definition for biometric recognition: "automated recognition of individuals based on their biological and behavioral characteristics."[3] This definition encompasses the two most common biometric processes: biometric verification (sometimes called "authentication") and biometric identification.

Verification compares an existing template of a biometric identifier to a newly submitted template to verify a person's identity, for example, using a finger scan or face template to unlock a mobile phone or clock into one's workplace. This process is referred to as 1:1 matching because the software compares the newly submitted information only with the stored information of the claimed identity.[4]

---

3. ISO/IEC 2382-37:2022 *Information technology — Vocabulary — Part 37*: *Biometrics*, ISO, https://standards.iso.org/ittf/PubliclyAvailableStandards/ (last visited May 10, 2024).

4. ANIL K. JAIN ET AL., INTRODUCTION TO BIOMETRICS, 10–11 (2011).

Identification compares a newly submitted biometric template to a database of stored templates to identify a person.[5] This process is used to prevent and detect alias or duplicate enrollments, whether accidental or intentional—called "scrubbing" for double identity holders—and by law enforcement to search for matches against criminal databases for background checks or in criminal investigations, among others.[6] Private commercial entities have similarly used facial recognition systems to identify individuals in a variety of contexts, including for security purposes.[7] This process is referred to as 1:n matching because the software compares the newly submitted information with a database containing the stored information of multiple other records.

Most biometric recognition systems follow a basic operating model that includes the following components:[8]

Acquisition and Enrollment: Software captures a raw data sample of a particular physical feature from an individual. Some biometric modalities typically require direct contact with a device to scan the feature. For example, finger scans capture a 2D image of the friction ridges present on the subject's finger pad. Others, such as facial recognition, can be acquired from a real-time camera image or by scanning existing other sources, such

---

5. *Id.* at 11–12.

6. 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.

7. *See, e.g.*, Tom Chivers, *Facial recognition . . . coming to a supermarket near you*, GUARDIAN (Aug. 4, 2019), https://www.theguardian.com/technology/2019/aug/04/facial-recognition-supermarket-facewatch-ai-artificial-intelligence-civil-liberties.

8. JAIN, *supra* note 4, at 3–10; BIOMETRIC SYSTEMS: TECHNOLOGY, DESIGN AND PERFORMANCE EVALUATION 9–14 (James Wayman et al. eds., 2005) [hereinafter BIOMETRIC SYSTEMS].

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 reflecting the unique landmarks derived from the subject's sample.

Liveness Detection: Liveness detection is a security countermeasure, used in some biometric recognition systems, that can be deployed to distinguish a biometric trait presented by a live person from an artificial submission of data. The type of liveness detection used will vary based on the biometric modality. Examples of liveness detection include pulse rate, blood flow, muscle contractions, electrical responses from human tissue, and three-dimensional variations in how the subject repositions between successive captures.[9]

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

Data Storage: The system retains a database of enrolled templates to search and compare, or the subject may carry its template in a secure form. The software typically associates each template with an identifier. In some cases, such as a digital electronic identification, the record with the enrolled template is placed on a phone or smartcard and is carried by the subject.

Data Matching: Software uses a computer algorithm to determine whether the new template is sufficiently similar to the

9. JAIN, *supra* note 4, at 272–78; *see also* Abdenour Hadid et al., *Biometrics Systems Under Spoofing Attack: An Evaluation Methodology and Lessons Learned*, 32 IEEE SIGNAL PROCESSING MAG. (Sept. 2015), at 20.

enrolled template(s) from the database or a personally carried medium to be considered a "match" for the purposes of the system's design and purpose. After a matching algorithm compares the similarities between the enrolled template or templates and the one presented for authentication, the resulting output can either be used to validate a claimed identity for verification purposes, or to rank matches across multiple identities for identification purposes. 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.[10]

System Parameters: Some systems allow the end-user/operator to define or modify the threshold requirements for determining when a new sample potentially "matches" the existing record or records based on the purpose of the system use and the accuracy of the technology.[11]

C. Common Biometric Modalities

The field colloquially described as "biometrics" continues to advance, with developers modifying existing technology and developing new ways to verify or identify individuals based on biological, physical, and behavioral characteristics. In addition, biometric systems increasingly use more than one characteristic, such as combining facial recognition with a finger scan, to take advantage of the different benefits of each and to increase the accuracy, security, and convenience of a system. Concerns about the risks of the use of various biometric characteristics for either identification or verification may change based on

10. JAIN, *supra* note 4, at 9–10.

11. ILEANA BUHAN & PIETER HARTEL, THE STATE OF THE ART IN ABUSE OF BIOMETRICS (2005).

whether a biometric system uses one or a combination of characteristics.[12]

Behavioral biometrics extend the use of biometric characteristics to create a unique profile of a distinctive behavior or 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 the person's identity.[13] These patterns often are combined with other information such as a person's IP address and/or location to identify suspicious authentication attempts that the system either blocks or triggers the requirement for an additional authentication method.

This section analyzes four of the physical characteristics most often used in biometric recognition systems to illustrate how different characteristics, and combinations of characteristics, offer distinctive benefits and pose different risks[14] The four characteristics we include—fingerprint, facial, iris, and voice recognition—generally illustrate the range of benefits and risks of using other characteristics, such as vein and gait recognition, though the use of existing biometric characteristics and the addition of new characteristics continue to evolve.

These benefits and risks vary to some extent for each characteristic. Incorporating multiple biometric characteristics and connecting one or more characteristics with other information further complicates the risk-benefit analysis of a biometric system. That calculus also depends on many other variables

12. JAIN, *supra* note 4, at 209–12.

13. *See* INT'L BIOMETRICS+IDENTITY ASS'N, BEHAVIORAL BIOMETRICS, https://www.ibia.org/download/datasets/3839/Behavioral (last visited May 10, 2024).

14. *See, e.g.*, WORLD BANK GROUP, TECHNOLOGY LANDSCAPE FOR DIGITAL IDENTIFICATION 18 (2018), https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf (identifying face, iris, and fingerprint recognition as "primary biometrics").

discussed below. This section illustrates the perhaps basic, but often overlooked, point that not all biometric characteristics are the same and underscores the importance of carefully considering those differences when selecting and designing biometric systems for different applications as well as whether a biometric system is the appropriate tool in the first instance.

1. Fingerprint Recognition

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*.[15] Galton cataloged unique characteristics, collectively called "minutiae," that collectively represented the various 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 minutiae. Although fingerprint analysts have identified as many as 150 different types of minutiae, only the points where ridges either terminate or bifurcate are considered salient for the purposes of automated recognition systems.[16]

During the enrollment phase, a subject places its 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 image needs

15. FRANCIS GALTON, FINGER PRINTS (1892).

16. Fed. Bureau Investigation, *Fingerprint Recognition*, https://ucr.fbi.gov/fingerprints_biometrics/biometric-center-of-excellence/files/fingerprint-recognition.pdf (last visited May 10, 2024).

to be processed before it can be used to identify minutiae points. First, the grayscale image is converted to a pure black-and-white image with no intermediate grays and is "thinned" to reduce each ridge down to the width of a single pixel. The system then identifies minutiae points by their orientation and coordinates on an x/y plane.[17] 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 its 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.

The threshold of similarity required to be deemed a "match" can be calibrated by the system designer or, in some instances, the system user to balance the risks of false rejection and false acceptance to find an appropriate matching threshold for the purpose and technology involved.

2. Facial Recognition

Generally speaking, facial recognition technologies can be divided into two distinct categories, which in turn consist of numerous competing subcategories.

The first 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 system first develops an average of all the face images in its dataset. Then, the system compares each

17. Lukasz Wieclaw, *A Minutiae-Based Matching Algorithms in Fingerprint Recognition Systems*, 13 J. MED. INFORMATICS & TECHS. 65 (2009); Ravi. J et al., *Fingerprint Recognition Using Minutia Score Matching*, 1(2) INT'L J. ENG'G SCI. & TECH. 35 (2009).

individual face image in that base set to the average, subtracting out the common elements they share and assigning mathematical weights to those variances. These mathematical representations of how a given face differs from the average in the set are called "eigenfaces," named after the concept of "eigenvectors" in linear algebra. New images are processed in the same way and are ranked based on how closely their eigenface transformations align with those that have already been calculated. If a certain characteristic combination of eigenfaces is substantially similar to a known image, then there is a mathematical basis to conclude the two images are visually similar.[18]

The second category ("Category 2") includes approaches (such as measurements of facial geometry) that identify distinguishing features of each subject's face. This model-based face recognition approach enables matching for facial images that do not share the same pose or orientation by constructing a facial graph from key landmarks such as corners of the eyes, tip of the nose, corners of the mouth, and chin.[19]

Category 1 technologies described above are "template-based" approaches that distinguish individual faces from a given, closed, set of data points. These approaches generally depend on comparing templates within a specific defined dataset and are amenable to security protections in their design that minimize the risk that the data could be used outside of the specific application.[20]

Category 2 methods create facial models that do not depend on replicating the orientation and lighting of the enrolled

18. Matthew Turk & Alex Pentland, *Eigenfaces for Recognition*, 3 J. COGNITIVE NEUROSCIENCE 71 (1991).

19. JAIN, *supra* note 4, at 122–24.

20. Yi C Feng et al., *A Hybrid Approach for Face Template Protection*, 6944 SPIE PROC: BIOMETRIC TECH. FOR HUM. IDENTIFICATION V (2008).

template and can potentially be used outside the original enrolled setting. These technologies are feature-based approaches that begin with measurements of specific facial features and their relationship to one another on a given face. Once a prominent orienting facial landmark (typically, the center of the eyes) is identified, the software crops out nonfacial components (such as hair) 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.[21]

In both categories of facial recognition technology, a visual image of a subject's face is processed to standardize and equilibrate the visual details. Further processing is performed on the standardized data to identify and extract the facial features relevant to the approach the system uses and store a mathematical representation of the significant features: eyes, nose, mouth, etc. (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 administrators of such systems can configure the threshold level of confidence for a match to be accepted and thereby balance the rate of false positives to false negatives based on the use case.

3. Iris Recognition

The iris is a thin diaphragm in the middle of the eye, situated behind the cornea and in front of the lens. The iris is composed of a complex set of muscles, tissue, blood vessels, and other biological structures that collectively have a distinct visual

21. R. Sivapriyan et al., *Analysis of Facial Recognition Techniques*, 57 MATERIALS TODAY: PROC. 2350 (2022), https://doi.org/10.1016/j.matpr.2022.01.296.

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.[22]

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.[23]

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 captured). 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

22. Richard Wildes, *Iris Recognition*, *in* BIOMETRIC SYS: TECH., DESIGN & PERFORMANCE EVAL., *supra* note 8, at 65–68; JAIN, *supra* note 4, at 141–45, 170–71.

23. Wildes, *supra* note 22, at 67.

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 the coordinates measured from the unwrapped iris, using algorithms to mathematically calculate a binary code called an "iris signature" that contains the 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.[24]

4. Voice Recognition[25]

Voice recognition technology proceeds from the assumption that each person's vocal tract is biologically unique, and therefore attributes of the speaker's voice are particular to that tract. The acoustic patterns of the speaker's voice are directly affected by the physical characteristics of the speaker's vocal tract, mouth, nasal cavities, jaw, tongue, larynx, and other biological features.[26]

Unlike some of 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

24. *Id.* at 73–86; JAIN, *supra* note 4, at 144–45.

25. As discussed in Part IV, several biometric information privacy statutes use the term "voiceprint," which may be distinct from "voice recognition."

26. M. M. Kabir et al., *A Survey of Speaker Recognition: Fundamental Theories, Recognition Methods and Opportunities*, 9 IEEE ACCESS *79236* (2021).

recognition is the only biometric modality available to authenticate a person's identity.[27]

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 or templates. The software compares the vector states to determine a statistical likelihood that the two samples come from the same speaker.[28]

27. Fed. Bureau Investigation, *Speaker Recognition*, https://ucr.fbi.gov/fingerprints_biometrics/biometric-center-of-excellence/files/speaker-recognition.pdf (last visited May 10, 2024).

28. Clark D. Shaver & John M. Acken, *A Brief Review of Speaker Recognition Technology*, PROC. 6TH INT'L MULTI-CONF. ON COMPLEXITY, INFORMATICS & CYBERNETICS: IMCIC 2015, at 172, http://archives.pdx.edu/ds/psu/19320.

III. BIOMETRIC SYSTEM BENEFITS AND DRAWBACKS

A. Benefits

Biometric systems can provide a variety of operational and security benefits across different settings. Most prominently, biometric technology can allow for enhanced security and protection of information, including sensitive personal information, through the use of biometric data as an access gateway in place of passwords or personal information (e.g., social security numbers) that can be forgotten, stolen, or shared.[29] To realize these benefits, designers of biometric recognition systems typically use characteristics that meet the following criteria:

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

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

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

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

Acceptable: Individuals do not generally object to having it measured or scanned.[30]

The growth of biometric technology is due, in part, to the potential for biometric systems to provide more secure, faster, cheaper, simpler, frictionless, and more user-friendly alternatives to other forms of information security. In "real world" scenarios, humans routinely rely on biological features to identify one another. Known associates can be recognized in one-on-one interactions by face or voice, while government-issued

29. Irfan Iqbal, *Biometrics: Security Issues and Countermeasures*, 4 INT'L J. SCI. & RES. 2229 (2015).

30. BIOMETRIC SYSTEMS, *supra* note 8, at 3–4.

identification cards provide photographs to facilitate the official verification of one's identity to a stranger. The use of biometric technology provides a mechanism to adapt this process into an electronic realm.

Proponents of biometric identification and authentication technologies note that it offers significant security advantages over other methods of information security. For example, reliance on passwords introduces a range of risks—from the use of weak or easily guessable passwords, to the ease with which passwords can be shared among other users in ways that reduce the security of the overall system and limit the ability to reliably identify individual users. From a security standpoint, biometrics are preferable over passwords because they aim to tie the authentication process directly to the actual subject's identity, rather than a password or token that can be forgotten, lost, or swapped. The aspects that make biometric-based security more secure are also aligned with ease of use.[31]

Instead of relying on a user to remember and protect different passwords, the person physically presents their persistent physical features to an electronic system to gain access. Because the templating technology in each system is often proprietary, the individual templates derived from persistent biological or behavioral features cannot be easily replicated even with access to a publicly available feature, like a person's face. Whereas a person who uses the same "password123" in multiple systems is exposed in all of them when that password is leaked, a person who is authenticated into multiple systems with a biometric,

31. David Kalat, *You Can't Change Your Fingerprints, But Do You Need To? The Evolution of Biometric- and Password-Based Authentication Security—Part I*, 5 PRATT'S PRIV. & CYBERSECURITY L. REP. 137 (2019); David Kalat, *You Can't Change Your Fingerprints, But Do You Need To? The Evolution of Biometric- and Password-Based Authentication Security—Part II*, 5 PRATT'S PRIV. & CYBERSECURITY L. REP. 217 (2019).

depending on the engineering of the affected systems, would not necessarily be exposed in all of them even if a template from one were to be leaked.[32]

Biometric recognition systems also play a prominent role in Multi-Factor Authentication (MFA). MFA is a security control that requires two or more forms of authentication to confirm identity. MFA has long been recognized as a best practice for data security, and federal and state regulators increasingly require it. For example, beginning in 2021, all federal agencies are required by an executive order to use MFA, and the New York Department of Financial Services Cybersecurity Regulation explicitly requires MFA in some circumstances.[33]

While all forms of MFA increase security, the Cybersecurity and Infrastructure Security Agency (CISA) recently released a fact sheet describing how phishing and similar attacks undermine several common types of MFA, including SMS (Short Message Service, i.e., standard text messages) and voice messages, and calling on organizations to implement "phishing-resistant" forms of MFA.[34] CISA noted that the only widely available form of phishing-resistant MFA is the Fast ID Online/Web Authentication standard developed by the FIDO Alliance and published by the World Wide Web Consortium ("FIDO2").[35] The FIDO2 standard uses either separate physical tokens or biometrics to confirm a user's identity.

---

32. *Id.*

33. *See* Exec. Order No. 14028, 86 C.F.R. 26633 (2021); 23 N.Y. FIN. SERV. LAW § 550.12 (McKinney 2023).

34. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, IMPLEMENTING PHISHING-RESISTANT MFA 3–4 (2022), https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

35. *Id.*; *How FIDO Works*, FIDO ALL., https://fidoalliance.org/how-fido-works/ (last visited May 10, 2024).

The Federal Trade Commission (FTC) has also identified phishing-resistant MFA as an element of the reasonable security required for organizations that collect consumer data. In two recent settlements with companies over lax security practices, the FTC ordered both organizations to adopt MFA methods and specifically prohibited using telephone or SMS-based authentication.[36]

B. Drawbacks

Critics of biometric technologies and academics studying these issues have voiced concerns that the reliable and persistent link to an individual that makes biological characteristics (like face, iris, fingerprint, and voiceprint) useful for recognition also can be viewed as an intrusion into one's personal space and privacy—and a challenge to the autonomous control of personal information.[37]

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

---

36. Decision and Order at 6, Drizly, LLC, FTC Docket No. C-4780 (Jan. 10, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Decision-and-Order.pdf; Decision and Order at 5–7, Chegg, Inc., FTC Docket No. C-4782 (Jan. 25, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Decision-and-Order.pdf.

37. *See, e.g.*, BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES 11 (Joseph Pato & Lynette Millett, eds., 2010); ELEC. FRONTIER FOUND., *supra* note 2.

data in an unexpected way.[38] Such concerns may be compounded by the reality that some biological features, like a person's face, are often publicly available, potentially facilitating the identification of an individual or the aggregation of their data without the subject's knowledge.

Consequently, some privacy advocates have argued that compromised biometric information from one system could be used to steal a person's identity across multiple systems that rely on the same biometric feature, or that biometric features could be used to combine data about an individual, de-anonymize it, or share it with multiple entities.[39] The following list identifies and briefly explains some of the key privacy and related concerns that have been raised in the collection and use of biometric information.

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

This concern is heightened by the risk that a persistent biological characteristic could be aggregated with other sources of personal information to form a more detailed profile of an

38. *See, e.g.*, IDENTIFICATION FOR DEVELOPMENT, A PRIMER ON BIOMETRICS FOR ID SYSTEMS (2022) 31–32 (ID4D).

39. *Id.*

individual.[40] Any collection of personal information raises this risk. But unlike information linked by a name, a credit card number, or an IP address, for example—where the link to an individual could be broken—the relatively immutable nature of the biological characteristics used in biometric systems raises concerns that the link may be unchangeable, i.e., data will be permanently associated with one's actual identity.

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

Security. Advocates of biometric technologies argue that such systems offer improved security to verify identity because the biological characteristics used are intimately connected to an individual and often must be physically presented for verification.[41] Biometric systems are not, however, immune from compromise.

Biometric systems approximate whether a new template (i.e., biometric input) sufficiently matches the existing one. Attackers can spoof a system by using techniques such as downloading or printing a person's photo, using a fake silicone

40. AI NOW INSTITUTE, REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS 7–8 (Amba Kak ed., September 1, 2020), https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions.

41. Iqbal, *supra* note 29.

fingerprint, or using a 3D mask. Such attacks are known as presentation attacks.[42]

Moreover, recent research has demonstrated the possibility of generating both "master prints" and "master faces" that match the partial fingerprints and faces of multiple people and could therefore theoretically give access to a large number of user accounts for multiple individuals.[43] At present, this risk is remote and limited to systems that use multiple enrollments for the same biometric.

The security of stored biometric information is itself a key consideration. If that information has the potential to be used across multiple systems, compromise of it creates a far greater security risk than a compromised password or other identifier that can be changed.[44]

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

42. *See* Hadid et al., *supra* note 9.

43. *See* Aditi Roy et al., *MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems*, 12(9) IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY 2013 (2017), https://ieeexplore.ieee.org/document/7893784; Ron Shmelkin et al., *Generating Master Faces for Dictionary Attacks with a Network-Assisted Latent Space Evolution*, 2021 16TH IEEE INT'L CONF. ON AUTOMATIC FACE & GESTURE RECOGNITION (2021), https://ieeexplore.ieee.org/document/9666968.

44. *See* A PRIMER ON BIOMETRICS FOR ID SYSTEMS, *supra* note 38.

the individual) that allow for the covert collection of information.[45]

Secondary Information. Templates from some biometric systems can contain secondary information that could be harvested and used beyond the individual's knowledge or consent. For example, some systems claim to be able to detect emotions and other information from both static and live facial images.[46]

Tracking and Surveillance. Identifying individuals by means of biometric information expands the ability to track the movement, activity, and behavior of those individuals. This is particularly the case with biometric information that can be implemented surreptitiously—most notably, facial recognition technologies.[47]

Function Creep. Function creep involves the reuse of sensitive information beyond the purpose for which it was originally collected. Function creep can occur with benevolent intent. For example, in Australia, a biometric database originally designed to prevent cross-border criminal activity was used to identify individuals who lost other forms of identification in brushfires and provide them aid.[48] But it may also compound potential

45. *See, e.g.*, YAMILA LEVALLE, BYPASSING BIOMETRIC SYSTEMS WITH 3D PRINTING AND 'ENHANCED' GREASE ATTACKS, DREAMLAB TECHS. (2020), https://dreamlab.net/media/img/blog/2020-08-31-Attacking_Biometric_Systems/WP_Biometrics_v5.pdf.

46. *See, e.g.*, *TechDispatch #1/2021 – Facial Emotion Recognition*, EUR. DATA PROT. SUPERVISOR (May 26, 2021), https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12021-facial-emotion-recognition_en.

47. *See* ELEC. FRONTIER FOUND., *supra* note 2.

48. Justin Hendry, *Services Australia put face matching to work for bushfire relief payments*, ITNEWS (June 5, 2020), https://www.itnews.com.au/news/services-australia-put-face-matching-to-work-for-bushfire-relief-payments-548978.

concerns about identity theft, tracking, the collection or sharing of personal information, and misidentification, particularly as the use of biometrics evolves and becomes more predominant.

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

Function creep also can affect security. Using biometric data for new purposes often means increased access, storage points, and potential disclosure of that data. Likewise, the quality and integrity of biometric data require examination when function creep arises—the integrity of biometric data suitable for one purpose (e.g., home security) may not be suitable for a new purpose (e.g., criminal identification by law enforcement) and may result in misidentification or security flaws.[49]

The potential for private biometric systems to share information with law enforcement and national security agencies intensifies these concerns. In 2015, the FBI announced that it would start to retain fingerprints submitted for routine background checks in its searchable criminal database.[50] A series of U.S. House and Senate investigations into law enforcement access to private biometric databases have highlighted the sometimes blurred lines between private and public use of biometric

49. *See* A PRIMER ON BIOMETRICS FOR ID SYSTEMS, *supra* note 38, at 31–32.

50. Jennifer Lynch, *FBI Combines Civil and Criminal Fingerprints into One Fully Searchable Database*, ELEC. FRONTIER FOUND. (Sept. 18, 2015), https://www.eff.org/deeplinks/2015/09/little-fanfare-fbi-ramps-biometrics-programs-yet-again-part-1.

information and even prompted legislation.[51] These and other examples demonstrate the ease with which private biometric information can be obtained and shared with law enforcement.[52]

Discrimination and Bias. Critics of biometric systems and other algorithm-based decision systems have noted patterns of discrimination against certain groups, which can result in perpetuating and exacerbating existing discriminatory structures or processes.[53] 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 such as race, sex, and age than other biometric modalities such as fingerprints and irises.[54]

---

51. *See* Letter from Sen. Edward J. Markey to Founder and CEO of Clearview AI, Hoan Ton-That (June 8, 2020), https://www.markey.senate.gov/download/clearview-ai-protests-letter; Fourth Amendment Is Not For Sale Act, 117th Cong. § 1265 (2021).

52. *See, e.g.*, Nicol Turner Lee & Caitlin Chin-Rothmann, P*olice Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color*, BROOKINGS (Apr. 12, 2022), https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.

53. *See, e.g.*, Davide Castelvecchi, *Is Facial Recognition Too Biased to Be Let Loose?*, NATURE (Nov. 18, 2020) https://www.nature.com/articles/d41586-020-03186-4. For a broader discussion of these issues, *see* CHRISTIANE WENDEHORST & YANIC DULLER, BIOMETRIC RECOGNITION AND BEHAVIOURAL DETECTION: ASSESSING THE ETHICAL ASPECTS OF BIOMETRIC RECOGNITION AND BEHAVIOURAL DETECTION TECHNIQUES WITH A FOCUS ON THEIR CURRENT AND FUTURE USE IN PUBLIC SPACES, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs (2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf.

54. Christian Rathgeb et al., *Demographic Fairness in Biometric Systems: What Do the Experts Say?* 41(4) IEEE TECH. & SOC'Y MAG. 71, (Dec. 2022), https://ieeexplore.ieee.org/document/9975333.

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).[55] From a technical performance perspective, it is relatively straightforward to measure and quantify how a system performs on a specific metric across different demographics.[56] For example, the National Institute of Standards and Technology (NIST) has engaged in ongoing performance testing comparing several facial recognition algorithms against trained human reviewers. This Facial Recognition Verification Testing program, with some notable exceptions, has reported higher error rates for some demographic groups for both verification (1:1 matching) and identification (1:n matching), although the studies indicate that the systems are improving over time.[57]

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

Transparency. The risk of discrimination is exacerbated by the frequent lack of transparency in the deployment of these systems and the alleged use of privately created "watch list"

55. *Id.*

56. *Id*.

57. *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NAT'L INST. STANDARDS & TECH. (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

databases.[58] 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 no opportunity to contest it.[59] 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.[60]

58. *See* AI NOW INSTITUTE, *supra* note 40, at 11; Anshul Kumar Singh & Charul Bhatnagar, *Biometric Security System for Watchlist Surveillance*, 46 PROCEDIA COMPUT. SCI. 596 (2015).

59. Written Testimony of Meredith Whittaker to U.S. House Committee on Oversight and Reform, Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy 4 (Jan. 15, 2020), https://www.congress.gov/116/meeting/house/110380/witnesses/HHRG-116-GO00-Wstate-WhittakerM-20200115.pdf.

60. In 2021, Apple was sued by a black man who was misidentified as a shoplifter by one of its retail store's facial recognition security systems. *See* Kim Hart, *Facial recognition surges in retail stores*, AXIOS (July 19, 2021), https://www.axios.com/facial-recognition-retail-surge-c13fff8d-72c6-400f-b680-6ae2679955d4.html.

IV. U.S. BIOMETRIC PRIVACY LEGAL LANDSCAPE

A. Overview

In the U.S., biometric-specific regulation falls roughly into two phases. The first began in 2008 when Illinois passed the groundbreaking Biometric Information Privacy Act (BIPA).[61] Texas adopted a similar law in 2009.[62] In the second wave, several state and local governments passed laws targeting biometric information,[63] and a growing number of states have passed comprehensive consumer data privacy laws that specifically protect biometric information, often including it within a category of highly sensitive personal information.[64] Several other states include biometric information among the types of

61. 740 ILL. COMP. STAT. 14/1–99 (2023). BIPA provides for a private right of action, permitting "aggrieved" individuals to assert claims for violations of the statute. *Id*. at 14/20.

62. TEX. BUS. & COM. CODE ANN. § 503.001 (West 2023) (Capture or Use of Biometric Identifier). Unlike BIPA, The Texas statute does not provide for a private right of action.

63. *See, e.g.*, WASH. REV. CODE § 19.375.020 (2023) (Enrollment, disclosure, and retention of biometric identifiers; effective 2017); N.Y COMP. R. & REGS. Tit. 22, §§ 1201–1205 (McKinney 2023) (Biometric Identifier Information; effective 2021); PORTLAND, OR., CITY CODE ch. 34, §§ 10.010–10.050 (2022) (Digital Justice; Prohibit the use of Face Recognition Technologies in Places of Public Accommodation by Private Entities in the City of Portland; enacted 2020, effective 2021).

64. *See, e.g.*, California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2023) (amended by the California Privacy Rights Act, by vote in 2020, effective 2013, to address biometric information); Colorado Consumer Protection Act, COLO. REV. STAT. §§ 6-1-713, 6-1-713.5 (2023); Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1301-6-1-1313 (2023) (effective July 1, 2023); Maryland Personal Information Protection Act, MD. CODE ANN., COM. LAW §§ 14-3501 to 14-3508 (LexisNexis 2023) (amended 2018); Virginia Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575 to 59.1-585 (2023) (effective 2023); Tennessee Information Protection Act, Tenn. Pub. Acts 408 (effective July 1, 2025).

covered information in their data protection and breach notification laws.[65] Numerous states are considering biometric privacy legislation.[66]

At the federal level, members of both the House and Senate have introduced several unsuccessful legislative proposals to regulate biometric privacy, including through general data privacy laws.[67] The FTC's general consumer protection authority

---

65. *See, e.g.,* Arkansas Personal Information Protection Act, ARK. CODE ANN. §§ 4-110-101 to 4-110-108 (2023) (amended to address biometric data in 2019); DEL. CODE ANN. tit. 6, § II-12B-100-104 (2023) (Computer Security Breaches); IOWA CODE §§ 715C.1-2 (2023) (Personal Information Security Breach Protection); VT. STAT. ANN. Tit. 9, §§ 2430-2445 (2023) (Protection of Personal Information); WIS. STAT. § 134.98 (2023) (Notice of unauthorized acquisition of personal information).

66. *See, e.g.,* S.B. 1238, 2003 Leg., 1st Sess. (Ariz. 2023) (biometrics identifiers; collection; retention; disclosure); Kentucky Biometric Identifiers Privacy Act, H.B. 483, 2023 Gen. Assemb., Reg. Sess. (Ky. 2023); H.B. 0033 and S.B. 0169, 2023 Gen. Assemb., Reg. Sess. (Md. 2023) (Commercial Law – Consumer Protection – Biometric Data Privacy); H.B. 63, 193d Gen. Ct., 2023 Reg. Sess. (Mass. 2023) (An Act to protect biometric information); S.B. 195, 193d Gen. Ct., 2023 Reg. Sess. (Mass. 2023) (An Act to protect personal biometric data); S.B. 30, 193d Gen. Ct., 2023 Reg. Sess. (Mass. 2023) (An Act relative to protecting sensitive information under the security breach law); S.B. 954 & H.B. 2532, 2023 Leg., 93d Reg. Sess. (Minn. 2023) (A bill for an act relating to private data; establishing standards for biometric privacy; establishing a right of action); Biometric Information Privacy Act, H.B. 1047 & H.B. 1225, 102d Gen. Assemb., 1st Reg. Sess. (Mo. 2023); Biometric Privacy Act, A.B. 1362 & S.B. 4457, 2023-2024 Leg., 246th Reg. Sess. (N.Y. 2023); S.B. 2390, 2023-2024 Leg., 246th Reg. Sess. (N.Y. 2023) (Relates to prohibiting private entities from using biometric data for any advertising, detailing, marketing, promotion, or any other activity that is intended to be used to influence business volume, sales or market share, or to evaluate the effectiveness of marketing practices or marketing personnel); H.B. 121, 2023 Gen. Assemb., 77th Sess. (Vt. 2023) (An act relating to enhancing consumer privacy).

67. *See, e.g.,* Facial Recognition and Biometric Technology Moratorium Act of 2021, S. 2052, 117th Cong. (2021); National Biometric Information Privacy

over data privacy and security encompasses biometric information, and the FTC recently issued a policy statement directed to the "increasing use of consumers' biometric information" and warning that false or unsubstantiated claims about the accuracy or efficacy of biometric information technologies or about the collection and use of biometric information may violate the FTC Act.[68] Sector-specific laws, most prominently the Healthcare Insurance Portability and Accountability Act (HIPAA), also regulate some biometric information and/or practices related to that information.[69]

Government acquisition and use of biometric information is governed broadly by federal law. At the state and local levels, a growing number of ordinances regulate the acquisition of surveillance technologies and, more recently, ban the use of facial recognition. Recent proposals to expand the use of biometric systems by federal agencies have come under increased scrutiny and have even been reversed in some prominent cases.[70]

Act of 2020, S. 4400, 116th Cong. (2020); American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

68. *See* Press Release, Fed. Trade Comm'n, FTC Warns About Misuses of Biometric Information and Harm to Consumers: Agency Issues Policy Statement Addressing Emerging Technologies That Might Harm Consumers and Violate the FTC Act (May 18, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers.

69. *See* 45 C.F.R. § 164.512.

70. For example, the Internal Revenue Service reversed its decision to require taxpayers to verify their identities using a private facial recognition service, and the Department of Homeland Security rescinded a proposal to expand the use of biometric verification systems for people applying for immigration benefits. *See* Kimberly Adams and Jesus Alvorado, *About-Face: IRS to stop using ID.me to identify taxpayers*, MARKETPLACE (Feb. 8, 2022), https://www.marketplace.org/shows/marketplace-tech/about-face-irs-to-stop-using-id-me-to-identify-taxpayers; Saira Hussain, *Victory! Biden Administration Rescinds Dangerous DHS Proposed Rule to Expand Biometrics Collection*,

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. Nonetheless, a clear trend has emerged toward increased regulation of biometric information and systems and specifically to treat biometric information as sensitive personal information. To date, with the exception of some primarily local and county-level ordinances, U.S. biometric privacy laws do not entirely prohibit the private use of biometric technologies and/or collection, storage, and use of biometric information. Instead, these laws impose varying notice, consent, storage, and security requirements and limits on the sale, disclosure, and reuse of biometric information.

Notably, recent laws and proposed legislation uniformly treat biometric information as protected information, with some, including California's consumer data privacy law, requiring heightened protections.[71] A related set of laws and proposals require fairness, accountability, and transparency in the development and use of algorithms generally, including those used in biometric systems.[72] These developments all underscore the critical need to pay close attention to the legal and regulatory requirements both when deciding whether to adopt a biometric

---

ELEC. FRONTIER FOUND. (June 30, 2021), https://www.eff.org/deeplinks/2021/06/victory-biden-administration-rescinds-dangerous-proposed-rule-expand-biometrics.

71. *See*, *e.g.*, CAL. CIV. CODE § 1789.140 (West 2023) (defining "sensitive information" to include "The processing of biometric information for the purpose of uniquely identifying a consumer").

72. *See*, *e.g.*, *Legislation Related to Artificial Intelligence*, NAT'L CONF. OF STATE LEGISLATURES, https://www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx (Jan. 31, 2023) ("General artificial intelligence bills or resolutions were introduced in at least 17 states in 2022, and were enacted in Colorado, Illinois, Vermont and Washington. Colorado, Illinois and Vermont created task forces or commissions to study AI.").

system and to ensure continued compliance for existing systems.

The following summary of existing U.S. biometric privacy laws highlights the most common requirements and key differences, with a focus on Illinois's BIPA. BIPA is the leading model for biometric-specific legislation and, because it contains a private right of action, is the most extensively litigated.

B. State Biometric Privacy Laws

1. Biometric/Covered Information Definition

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

The Virginia Consumer Data Privacy Act (VCDPA) similarly defines biometric information as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual."[73]

---

73. VA. CODE ANN. § 59.1-575 (2023). The Connecticut Data Privacy Act provides the same definition of "biometric data" as the Virginia law. *See*

California's law uses a different model. The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), defines biometric information broadly as any "physiological, biological or behavioral characteristics" that "is used or is intended to be used singly or in combination with each other or other identifying data, to establish individual identity."[74] The law 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.[75] 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.

The CPRA amendments to the CCPA also include biometric information processed "for the purpose of uniquely identifying a consumer" within the new category of "sensitive personal information" for which the law creates additional consumer rights.[76]

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

CONN. GEN. STAT. § 42-515(4) (2023) (effective July 1, 2023); *see also* Tennessee Information Protection Act, 2023 Tenn. Pub. Acts 408 (same; effective July 1, 2025).

74. CAL. CIV. CODE § 1798.140 (West 2023).

75. *Id*.

76. *Id*. § 1798.140(c) (West 2023).

Competing concerns about ambiguity and clarity in each of these models animate debate not only about effective legislation, but also compliance. This lack of clarity creates substantial risk for organizations that use applications that incorporate biological and behavioral features.

2. Exemptions from Biometric Regulation

Many biometric privacy laws, like other consumer privacy laws, 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. For instance, BIPA excludes financial institutions or their affiliates that are subject to Title V of the federal Gramm-Leach-Bliley Act (GLBA), as well as information subject to HIPAA and information collected, used, or stored in a healthcare setting.[77] Many laws also make exceptions for uses that are pursuant to a valid warrant or subpoena or in court proceedings.[78]

Washington's law provides for GLBA and HIPAA exemptions and also carves out use by a law enforcement officer acting within the scope of his or her authority.[79] The Washington law also applies only where the enrollment of the biometric data is for a "commercial purpose," notably exempting from coverage any use "in furtherance of a security purpose."[80] This would seem to carve out using biometric information to authenticate a user's identity as part of a security program.

The exemptions in the Texas law are narrower, carving out only voiceprint data retained by a financial institution or an affiliate of a financial institution under GLBA from the application

77. *See* 740 ILL. COMP. STAT. 14/10, 14/25(b), 14/25(c) (2023).

78. *See id.* 14/25(a).

79. *See* WASH. REV. CODE § 19.375.020(7), 19.375.040 (2023).

80. *Id.* § 19.375.020(7).

of the statute.[81] The Texas statute also applies only where the data is captured for a "commercial purpose."[82]

California's CCPA includes similar exemptions for federal sector-specific privacy laws and also exempts from coverage any personal information, including biometric information, collected from publicly available sources.[83] But the law excludes from that exemption publicly available "biometric information collected by a business about a consumer without the consumer's knowledge."[84]

3. Notice and Consent Requirements

Most biometric privacy laws require notice and consent prior to use and/or disclosure, or allow consumers to opt out afterwards or from future disclosures. As with any new regulation, there are concerns about compliance with and enforcement of these procedures.[85]

---

81. TEX. BUS. & COM. CODE § 503.001(e) (West 2023).

82. *Id.* § 503.001(b) and (c).

83. CAL. CIV. CODE § 1798.140(o) (West 2023).

84. *Id*.

85. Although currently there is no comprehensive federal biometric data privacy law, the FTC recently settled an enforcement action under Section 5 of the Federal Trade Commission Act against a company related to its use of facial recognition technology. Decision and Order, Everalbum, Inc., FTC Docket No. C-4743 (May 6, 2021). According to the FTC's complaint, the company violated Section 5's prohibition of "deceptive acts or practices in or affecting commerce" by allegedly (1) promising to delete users' images if they deactivated their accounts, but in fact retaining the images and (2) suggesting on its website that it would only apply facial recognition technology to users' images with users' consent, but actually enabling the technology by default without many users' consent. *See* Press Release, Fed. Trade Comm'n, FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology (May 7, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse-facial-recognition-technology.

For example, BIPA requires written notice that biometric identifiers or information are being collected or stored, including notification of the "specific purpose and length of term" for the collection and storage. BIPA also requires a written release from the user prior to the collection or receipt of the biometric identifiers or information.[86]

As noted above, the CCPA as amended by CPRA lists biometric information as a special subcategory of personal information, called "sensitive personal information."[87] The law imposes several requirements on businesses that collect all forms of personal information, including that a business provide notice of what information it collects, whether it sells or shares that information, the length of time it intends to retain that information, and consumers' rights with regard to that information.[88] For sensitive personal information, a business also must

86. 740 ILL. COMP. STAT. 14/15(a), (b) (2023).

87. CAL. CIV. CODE § 1798.140(c) (West 2023).

88. *E.g.*, *id.* § 1798.100(a) (business that controls the collection of personal information must inform consumers at or before the point of collection regarding, e.g., categories of information collected, purposes of collection, length of time the business intends to retain each category of personal information); *id.* § 1708.105(b) (business shall disclose consumer's right to request the deletion of personal information); *id.* § 1798.106 (business shall disclose consumer's right to request correction of inaccurate personal information); *id.* § 1798.121(a) (business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in 1798.121 must notify consumers of use or disclosure and that consumers have the right to limit the use or disclosure of their sensitive personal information); *see id.* § 1791.130 (other provisions regarding Notice, Disclosure, Correction, and Deletion Requirements); § 1791.135 (additional provisions regarding disclosure and consent in the context of Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Personal Information); *see also, e.g.*, *id.* § 1798.110(c) (information required to be disclosed to consumers upon request).

disclose the purposes for the collection.[89] The CCPA further requires that collection, use, and retention of personal information be "reasonably necessary and proportionate" to achieve those purposes.[90] The CCPA limits some notice obligations when a consumer's sensitive personal information is being used for certain permitted purposes, including ensuring security and integrity and verifying a consumer's information.[91] This arguably could permit a business to use biometric information for authentication purposes without providing consumers a notice of their right to limit those uses, but only if the business uses the biometric information solely for such purposes and the business meets the statute's other notice and use requirements.[92]

Like the CCPA, the VCDPA includes biometric data within a category labeled "sensitive information." But the VCDPA goes further than California by prohibiting collection and processing of biometric data unless a business obtains "freely given, specific, informed, and unambiguous agreement" from the consumer.[93]

Colorado's Privacy Act mirrors Virginia's heightened consent requirement and also specifically prohibits obtaining consent by: (1) "[a]cceptance of a general or broad terms of use"; (2) "[h]overing over, muting, pausing, or closing a given piece of content"; and (3) and "[a]greement obtained through dark patterns."[94]

---

89. *Id*. § 1798.140(c).

90. *Id*. § 1798.100(a).

91. *See id*. §§ 1798.121(a), 1798.140(e)(2), 1798.140(e)(4), 1798.140(e)(5), 1798.140(e)(8).

92. *See id*.; *see also*, *e.g.*, *supra* note 64.

93. VA. CODE ANN. § 59.1-575 (2023).

94. COLO. REV. STAT. § 6-1-1303 (2023) (effective July 1, 2023).

The Washington law requires disclosure given "through a procedure reasonably designed to be readily available to affected individuals" prior to enrolling a biometric in a database.[95] The law specifies that the "exact notice and type of consent required to achieve compliance . . . is context-dependent" but is something less than affirmative consent.[96] 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."[97]

4. Sale and Disclosure of Biometric Data

Current and proposed laws address the sale and disclosure of biometric data by prohibiting or restricting the sale or profiting from biometrics as well as placing restrictions on their disclosure. For example, BIPA requires notice and prior consent for any disclosure of biometric data to a third party.[98] Moreover, BIPA prohibits "private entit[ies] in possession of a biometric identifier or biometric information" from selling, leasing, trading, or "otherwise profit[ing]" from a person's biometric identifiers or biometric information.[99] The scope and application of this provision, however, remains unclear. For example, some argue that a private entity that sells a "biometric device" or hosts such data for a fee is "otherwise profiting" from a person's biometrics, while others contend such indirect "profiting" not involving the sale of biometric information is outside the scope of

95. WASH. REV. CODE § 19.375.020(2) (2023).

96. *Id*.

97. *Id.* § 19.375.020(5).

98. 740 ILL. COMP. STAT. 14/15(d) (2023); *see also* WASH. REV. CODE § 19.375.020(3) (2023) (permitting disclosure where necessary to provide a product or service explicitly requested by the individual).

99. 740 ILL. COMP. STAT. 14/15(c) (2023).

BIPA and prohibiting it would substantially curtail or eliminate the ability of companies to provide biometric technology or data hosting.

The CCPA lists biometric information as a category of sensitive personal information with heightened protections. A business that collects biometric information must "[p]rovide a clear and conspicuous link on the business' internet homepages" that will permit the consumer, or a person authorized by the consumer, to limit the use or disclosure of their information.[100] Consumers have the right to limit the use and disclosure of sensitive personal information to those purposes "necessary to perform the services or provide the goods reasonably expected by an average consumer" and for other specific purposes defined in the statute.[101]

5. Retention of Biometric Data

As discussed above, biometric data generally is considered personal information that may pose privacy and security concerns when collected and retained. Some biometric laws address retention requirements by imposing an upper limit on the retention period, pegged to the purposes or services for which the biometrics were collected.[102] Considerations for such laws

100. CAL. CIV. CODE § 1798.135 (West 2023).

101. *Id.* § 1798.121; *see also id.* § 1798.140(e)(2) (security and integrity), (4) (short-term, transient use), (5) (performing certain services on behalf of the business, including verifying customer information), (8) (verifying or maintaining the quality and safety of the business's service or device).

102. For example, BIPA requires a retention schedule and guidelines for destroying biometrics, both of which must be publicly available and allow 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 ILL. COMP. STAT. 14/15(a) (2023). The Texas law requires retention within a "reasonable period of time" but then caps that period at a year after there is no

include 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.

6. Enforcement and Penalties

Existing biometric privacy laws generally take one or both 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, allowing individuals to bring claims in court alleging their biometric data was collected, disclosed, or retained in violation of BIPA.[103] California provides a private right of action and statutory damages for the unauthorized access and exfiltration, theft, or disclosure of certain types of personal information, including unique biometric data if obtained together with a person's name.[104] Other states, like Texas and Washington, restrict enforcement to their respective state attorneys general.[105]

---

longer a valid reason for maintaining the biometric. TEX. BUS. & COM. CODE § 503.001(c)(3) (West 2023). Where the biometric serves the purpose of employee identification, then the biometric must be destroyed within a year after the employment relationship is terminated. *Id*. 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." WASH. REV. CODE § 19.375.020(4)(b)(i)-(iii) (2023).

103. 740 ILL. COMP. STAT. 14/20 (2023).

104. CAL. CIV. CODE § 1798.150 (West 2023).

105. WASH. REV. CODE § 19.375.030(2) (2023); TEX. BUS. & COM. CODE § 503.001(d) (West 2023).

These biometric privacy laws also provide for monetary penalties and other compensation. BIPA, for example, provides that the prevailing party "may recover" the greater of a specified liquidated damages or actual damages, as well as reasonable attorneys' fees and costs.[106] The statute of limitations for a BIPA claim is five years,[107] and claims under sections 15(b) and (d) accrue with each collection and disclosure of a person's biometric identifier or information,[108] leading to potentially staggering statutory damages. Other states provide a statutory cap per violation.[109]

7. Security

The current and proposed biometric-specific privacy laws typically impose general standards for data 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."[110] The Washington law requires "reasonable care."[111]

---

106. BIPA provides that a prevailing party "may recover" for each violation the greater of liquidated damages of $1,000 (negligent violations) or $5,000 (intentional or reckless violations) or the party's "actual damages." 740 ILL. COMP. STAT. 14/20(1) and (2) (2023). BIPA also provides that a prevailing party "may recover" reasonable attorneys' fees and costs. *Id*. 14/20(3).

107. Tims v. Blackhorse Carriers, Inc., 216 N.E.3d 845 (Ill. 2023).

108. Cothron v. White Castle Sys., Inc., 2023 IL 128004 (Ill. 2023).

109. For example, Texas caps civil penalties at $25,000 per violation. TEX. BUS. & COM. CODE § 503.001(d) (West 2023).

110. 740 ILL. COMP. STAT. 14/15(e) (2023); TEX. BUS. & COM. CODE § 503.001(c)(2) (West 2023).

111. WASH. REV. CODE § 19.375.020(4)(a) (2023).

General privacy laws that encompass biometrics also require a baseline level of security. For example, California's law permits private rights of action where a data breach results from a business's "violation of the duty to implement and maintain reasonable security procedures and practice appropriate to the nature of the information."[112]

The general trend in data security laws is toward more specific requirements, though there is debate whether that approach is appropriate given the rapidly evolving security threat landscape. For example, the NY SHIELD Act, which includes "biometric information" in its definition of "private information" regulated under the statute, requires reasonable safeguards to protect the security, confidentiality, and integrity of private information, including its disposal.[113] Likewise, the VCDPA requires data controllers to conduct and document a data protection assessment prior to processing biometric data.[114]

112. CAL. CIV. CODE § 1798.150 (West 2023).

113. Stop Hacks and Improve Electronic Data Security (SHIELD) Act, N.Y. GEN. BUS. LAW § 899-bb (McKinney 2023).

114. VA. CODE ANN. § 59.1-578 (2023).

V. SYSTEM SELECTION AND DESIGN

The legal issues identified above illustrate some of the risks posed by the use of biometric systems, but in most U.S. jurisdictions, existing laws address only a relatively small subset of the issues these systems raise or are perceived to raise. In addition, biometric systems incorporate advanced technologies, including algorithms, machine learning, and artificial intelligence, that also have come under increased regulatory scrutiny.[115]

More broadly, the collection of biometric information generally, and some biometric modalities in particular, like facial recognition, may pose reputational risks beyond legal liability. As a result, organizations considering implementing biometric systems and professionals advising those organizations should consider not only existing legal requirements and the likelihood that those requirements will change, but also the broader reputational risks that could arise from using these systems.

The process of selecting or designing biometric recognition systems presents organizations the opportunity to make intentional choices that can mitigate the risks these systems pose to users and the organizations implementing them. This section identifies several general considerations organizations should consider, including:

Biometric Modality: Each biometric modality offers different benefits and poses different risks that should be assessed in determining whether a system fits a specific application, including the legal, security, and privacy risks it poses relative to other modalities.

System Design and Accuracy: Accuracy depends on the entire system, not only the algorithm used in it. While generally

115. *See, e.g.*, Alex Engler, *The EU and U.S. are starting to align on AI regulation*, BROOKINGS (Feb. 1, 2022), https://www.brookings.edu/blog/techtank/2022/02/01/the-eu-and-u-s-are-starting-to-align-on-ai-regulation.

speaking, biometric systems across all modalities are increasingly accurate, the actual performance of each system will vary substantially depending on how it is configured and used.

Privacy and Nondiscrimination: Biometric information generally is treated as protected and sometimes sensitive information that implicates user privacy and discrimination concerns, which should be assessed and mitigated.

Security and Integrity: Protecting biometric data requires both security and integrity. A key element of both aspects is mitigating the risk that a biometric template could be reused across different systems and/or reverse-engineered to identify the original biological feature used to generate it.

A. Biometric Modality

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

It is equally important to recognize that each biometric modality offers a different mix of benefits and risks. For example, people's faces are a fundamentally public feature, commonly visible and exposed. This fact, coupled with the ability for technology to effectively perform facial recognition on photographs or surveillance video, regardless of whether the subject purposefully engaged in the recognition process, gives rise to a broad range of privacy concerns.[116] Those same features,

116. Privacy concerns regarding facial recognition will be addressed in a forthcoming companion publication, The Sedona Conference, *Commentary on Notice and Consent Principles for Facial Recognition Technology*.

however, also offer distinctive benefits, including the ability to conduct remote identity verification.[117]

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

As discussed above, biometric systems increasingly incorporate more than one modality. Among other things, a multimodal system can provide benefits including increased security, higher accuracy, and reduced bias. At the same time, by collecting two or more biometric features, such systems increase privacy, security, and related risks.

B. System Design and Accuracy

The accuracy of each biometric system varies significantly, largely depending on what aspect of system performance is measured. For example, a system may perform well when measuring the overall percentage of correct identifications but poorly when measuring its ability to correctly identify a single individual across multiple different photos. Accuracy also depends on quality of the hardware and software associated with

117. *Id.*

the system, as well as how a system is configured and used in a specific application.[118]

The following list identifies and briefly describes the most significant factors that can affect the accuracy of biometric systems. These factors operate together to determine the accuracy of a given biometric system.[119]

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

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

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

---

118. Generally speaking, the accuracy of biometric systems using the most common 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 NIST. *See NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, *supra* note 57.

119. *See generally*, BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES, *supra* note 37; A PRIMER ON BIOMETRICS FOR ID SYSTEMS, *supra* note 38, at 74.

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

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

One basic measure of the accuracy of a biometric system focuses on the rate of false matches ("false positives") and the rate of false nonmatches ("false negatives"). Each time a system captures a person's biometric, the resulting template will be different and can be different to varying degrees. The algorithm used in the data matching process therefore must estimate whether the new template is sufficiently similar to the stored one.

This means that calibrating a system's algorithm to accept a greater range of variability in the new template to reduce the number of false negatives will increase the number of false positives, and vice versa. The desired balance will vary depending on the specific technology and its individual implementation. For example, configuring a system to prioritize efficiency and access may require accepting a larger number of false positive identifications by permitting the system to accept a larger variation in templates. By contrast, prioritizing security requires accepting a larger number of false negatives to ensure that the system accepts only very closely matched templates.[120]

120. *See Biometric recognition and authentication systems: Measuring performance*, NATIONAL CYBER SECURITY CENTRE, https://www.ncsc.gov.uk/collection/biometrics/measuring-performance (last visited May 10, 2024).

ISO recognizes three kinds of biometric system evaluations: technology, scenario, and operational. NIST evaluations have documented increasing accuracy on technical evaluations for the top-performing systems in major modalities but also substantial differences among systems.[121] Scenario and operational testing are less common but are important to identify how systems work under the actual conditions in which a system operates. Even systems that incorporate algorithms that perform well under NIST's technical evaluations may perform less well in real-world conditions.[122] Independent scenario and operational testing of facial recognition systems has demonstrated that accuracy depends on the entire system configuration, including the quality of the equipment used to acquire images and the conditions under which they were created.[123]

C. Security and Integrity

Well-designed biometric systems emphasize process integrity as much as secrecy to ensure that the chain of custody from sample capture, comparison, and returning results are protected from tampering or manipulation, even by an imposter armed with stolen or publicly captured biometric data. It is impossible to comprehensively define the specific measures that meet the "reasonable security" standard that most biometric laws require. Nonetheless, as many of these laws treat biometric

---

121. *See NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, *supra* note 57.

122. *See* YEVGENIY SIROTIN & ARUN VEMURY, DEMOGRAPHIC VARIATION IN THE PERFORMANCE OF BIOMETRIC SYSTEMS: INSIGHTS GAINED FROM LARGE-SCALE SCENARIO TESTING, DHS SCIENCE AND TECHNOLOGY (2021), https://www.dhs.gov/publication/demographic-variation-performance-biometric-systems.

123. *See* Yevgeny Sirotin, *'Bias' in face recognition: some facts*, LINKEDIN (Oct. 16, 2019), https://www.linkedin.com/pulse/bias-face-recognition-some-facts-yevgeniy-sirotin-phd/.

data as sensitive, it is critical to develop an appropriate security program addressing the collection, storage, and use of biometric information. Multiple authorities, including ISO, a leading international standards body, identify the following elements for biometric information security that entities could consider adopting in whole or in part in developing their programs for biometric information security:[124]

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

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

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

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

One of the distinctive security challenges raised by biometric recognition systems is that the process of comparing stored templates to newly submitted input data is a process that requires direct access to the data in the template. Consequently, certain data protection techniques that rely on keeping sensitive data encrypted (for example, the use of hash functions, which are

124. JAIN, *supra* note 4, at 286–87; *see also* ISO/IEC 24745:2022, *Information Security, Cybersecurity and Privacy Protection—Biometric Information Protection*, INT'L STANDARDS ORG. (2022), https://www.iso.org/standard/75302.html (collapsing these into three security requirements for secure biometric systems: i) unlinkability and renewability; ii) irreversibility; and iii) performance preservation).

commonly used to protect passwords in an encrypted format) are inapplicable to biometric recognition systems. Instead, a well-designed biometric recognition system will deploy other techniques, in keeping with the principles above, to provide comparable protections.[125]

Securing a biometric system involves protecting both the algorithm used to create biometric templates as well as the templates the algorithm generates using "reasonable" security practices, which may include encrypted storage, appropriate access controls, and/or access logging and monitoring.[126] In addition, consideration should be given to segregating the algorithm used to create biometric templates from the templates themselves, as doing so may lower the risks that both aspects will be disclosed in a security incident, and thus the risk that the incident could allow an attacker to impersonate an individual.[127]

Perhaps most important in the biometric context, consideration should be given to whether the algorithm itself can and should be designed in a way such that it holds no value outside of the current system. One of the most common objections leveled against the use of biometric systems is that theft of a biometric template will irrevocably compromise a person's identity because it is impossible to change the underlying physical feature. A biometric system that uses a unique algorithm may ensure that if the algorithm is exfiltrated from that system, it cannot be used to reverse-engineer the biometric attributes of templates from another system.[128]

---

125. Anil K. Jain et al., *Biometric Template Security*, EURASIP J. ON ADVANCES IN SIGNAL PROCESSING (2008).

126. *See* Iynakaran Natgunanathan, et al., *Protection of Privacy in Biometric Data*, 4 IEEE ACCESS 880 (2016).

127. *Id.*

128. *See* A PRIMER ON BIOMETRICS FOR ID SYSTEMS, *supra* note 38, at 27–29; ISO/IEC 274745, *supra* note 124.

For the new and existing or enrolled templates, consideration should be given to employing security measures designed to protect against the injection of unauthorized templates.[129] In addition to the general measures just identified, a system's security might be further enhanced by including a method to validate the template against the specific algorithm that was used to create the template. Doing this may ensure that if an unauthorized template is injected into the biometric system, it cannot be used to validate unauthorized credentials, as the injected template would not validate against the specific biometric system algorithm. Note that if biometric system algorithms are designed such that they are proprietary to a given system and dissimilar to other system algorithms, then exfiltration of a protected template itself potentially has no value outside of the existing system and cannot be used on its own to reverse-engineer the biometric attributes of an individual.[130]

Integrating data integrity principles into the design of a biometric system also potentially ensures much greater security. Ensuring data integrity means establishing chain of custody and including data validation steps such as checksums when protected templates are created.[131] Data integrity implemented at the time of protected template creation may ensure 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 also can affect system accuracy, specifically as it relates to the balance between false positives and false negatives, which is dependent on the use of

129. ISO/IEC 274745, *supra* note 124.

130. A PRIMER ON BIOMETRICS FOR ID SYSTEMS, *supra* note 38.

131. ISO/IEC 247745, *supra* note 124.

the biometric system (verification, or 1:1 matching, vs. identification, or 1:n matching).

D. Privacy and Nondiscrimination

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

The modality selection and system design considerations outlined above can mitigate many of these concerns. For example, a modality such as a finger scan is far more difficult to use to publicly identify a person without their consent than facial or gait recognition. Likewise, using proprietary templates that are difficult to reverse-engineer protects individuals against the risk of identity theft in the case of unauthorized disclosure.

As noted above, an increasing number of jurisdictions impose specific legal requirements to protect biometric information. Most of these laws include consent requirements for obtaining biometric data and restrict how that data can be used and shared. They also impose specific retention requirements and, in some jurisdictions, like California, provide consumers with specific rights.

Organizations should also consider how their systems may directly or indirectly discriminate against different demographic groups. The risks here can arise in different ways, ranging from a system that is less accurate for different races,

genders, and ages to applications that are or may be deployed in ways that disproportionately affect specific demographic groups.