

The Sedona Conference WG11 Brainstorming Group Outline - Biometric Privacy Laws (September 2020)



Copyright 2020, The Sedona Conference.
All rights reserved.

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to comments@sedonaconference.org no later than November 1, 2020.

The Sedona Conference WG11 Brainstorming Group Outline – Biometric Privacy Laws

(September 2020)

Brainstorming Group Members:

Brian Ray (Brainstorming Group Leader)

Kate Baxter-Kauf

David Berger

Brett Doran

Arianna Evers

Glenn Friedemann

David Morrison

Ben Patton

Frank Nolan

Patrick Quirk

Dalia Ritvo

Meredith Schultz

Jim Sullivan

Douglas Swetnam

Starr Drum (Steering Committee Liaison)

Ruth Promislow (Steering Committee Liaison)

SEDONA CONFERENCE WG11 **BIOMETRIC PRIVACY LAW BRAINSTORMING GROUP OUTLINE**

I. INTRODUCTION

A. Background and Questions for Midyear Meeting Discussion

The WG11 Steering Committee provided the following mandate to this Brainstorming Group (BG) and tasked us with submitting a final outline on October 15. We completed this initial draft to generate discussion and solicit feedback from the WG11 group at the Midyear meeting. We will incorporate that feedback into the final draft.

B. Steering Committee Mandate

This BG should address the threshold question of whether it is desirable or necessary to have a set of uniform principles to guide the development of biometric privacy laws. To the extent the BG agrees that it is, the BG should consider the proposed parameters of a paper, identifying which principles or aspects of a biometric privacy law should be considered by the drafting team with a view to developing a recommended approach on those particular points. In setting out the proposed parameters of the paper and the work to be undertaken by the drafting team, the BG should consider the reasonable scope of issues that could be developed and finalized by a drafting team within a sufficient period of time for it to be a useful resource (i.e., before a large number of states develop biometric privacy laws).

The following are examples of potential issues that the BG may identify as worthy of analysis and a recommended uniform approach. The BG may identify other aspects of biometric privacy law principles that should be considered.

- What biometric data should be covered by a biometric privacy law? Should the law distinguish between biometric identifiers, such as fingerprints and voiceprints, and other types of biometric data, such as health or exercise data, or treat them uniformly?
- Should the law cover both private and government processing of biometric data? And, if so, how would the compliance requirements or use restrictions differ? For example, should there be consideration for emergency exercise of government authority and if so, what should be the guiding principles in the exercise of such emergency government authority?
- Should the law distinguish between or exempt certain processing contexts? E.g., financial fraud prevention/protection.
- What notice and/or consent requirements should there be? How do you ensure that the notice and consent provisions included are meaningful?
- How should the law address security protections for biometric data, including retention limits?

- How should enforcement and penalties be addressed? What should the balance be between regulatory and civil enforcement options?

C. Questions for the Midyear Meeting (or How to Skim our Very Long First Draft)

We decided at the beginning to keep as many issues on the table as possible and then try to come to some consensus on how to focus the final draft. We succeeded admirably at the first objective, and you will find a wealth of material below, including many sections that are developed to a depth not typical of a Brainstorm Outline.

Due, in part, to time, we have been less successful in achieving our second objective of producing a more focused outline for this draft.

You will see that we are recommending that a drafting group focus primarily on the issues related to private collection of consumer biometric data but with attention to the challenges in cleanly separating private and government collection. Beyond that, we have kept most of the other issues the group identified on the table for discussion, resulting in a very long list in Section VI.

As a result, we are keenly interested in suggestions/comments/reactions from the full WG11 group on: (1) possible ways to, as one of my law firm mentors used to say, “cut off the heads of the hydra” and focus the overall scope of the outline; and (2) more pointedly, input on which of the issues in Section VI to focus on in the final draft.

Which is a long-winded way of saying, if you are short on time and relatively familiar with the terrain, you might want to jump to Section VI.

II. AUDIENCE AND PURPOSE

This Outline assumes that a subsequent white paper would be directed primarily at legislators and policymakers. The Outline seeks to:

- provide a representative summary of major biometric privacy laws and industry principles, with a focus on the U.S. and the contested issues that these laws have raised;
- summarize representative examples of current biometric technology applications, likely future developments, and the benefits of these applications;
- analyze the privacy and civil liberties risks raised by these applications and how existing laws and policies have attempted to address these; and
- identify issues for which the drafting group should consider either developing consensus principles or, where consensus is not possible, recommending an analytical framework that policymakers could use to analyze the trade-offs involved in developing future legislation and regulations.

III. DEFINITIONS AND EXAMPLES OF BIOMETRIC DATA/TECHNOLOGIES

A. Biometric Modalities and Purpose

1. Biometrics are generally understood to encompass biological characteristics that make a person unique and allow for identification and/or verification of that individual. Biometrics involves recording unique physical, factual landmarks of a subject at enrollment, then later comparing a candidate's similarly acquired landmarks to determine a statistical match likelihood.

2. The public and private use of biometric technology is expanding dramatically. In 2018, the National Institute of Standards and Technology (NIST), which conducts periodic tests of facial recognition systems, emphasized that the technology was in the midst of an “industrial revolution,” as the top-scoring systems have improved more than 20 times over the systems it tested in 2014.¹ As the world adapts to COVID-19, the use of biometrics is expected to become more widespread in the public and private sectors alike.

3. The growth of biometric technology is due, in part, to the presumption that biometrics offer a more secure, faster, cheaper, simpler, and more user-friendly alternative to other forms of security, such as passwords and physical tokens. An additional benefit is protection against account takeover and unauthorized access delegation, preventing phishing and various forms of proxy fraud. Internet of Things (IoT) and edge computing devices as well as smart phones increasingly incorporate biometrics, and advances in artificial intelligence (AI), including neural networks, will contribute to the widespread adoption of biometrics.

4. Biometric data is collected on both a voluntary and involuntary basis, with and without consent from the subject (or “owner” of the biometric information), and with and without specific disclosure to the subject as to what will be done with the information, how it will be maintained, and whether it will be shared.

5. The rapid growth of these technologies has prompted growing concerns over the privacy, security, and civil liberties risks they raise, prompting a range of regulatory and policy responses and proposals including bans on governmental and police use of facial recognition technology in some communities, legislative proposals at the state and federal levels, and industry proposals for self-regulation.

B. Lack of Definitional Clarity and Evolving Technology

1. There is a lack of consensus as to what constitutes “biometric information,” “biometric identifier,” and/or “biometric data,” and there are competing definitions and terms used in the industry and in existing and proposed laws. New kinds or combinations of identifiers also emerge as technology develops. Typically, there is a distinction between the raw input data (e.g., a photo, fingerprint image, or voice recording), and the biometric template of landmarks generated from the raw data by an algorithm. Given a subject's raw input data, an algorithm can reproduce biometric templates, so possessing raw data is tantamount to possessing

¹ Patrick Grother, et al., *Facial Recognition Vendor Test (FRVT): Part 3: Demographic Effects*, NISTIR 8280 (2019), 15.

a biometric, and the opportunity to observe a subject in public presents the opportunity to collect the raw data. This reinforces the fact that biometric system integrity protections cannot be based on an assumption of secrecy.

2. In addition to unique biological characteristics such as facial structure, DNA fingerprints, finger/hand geometry, eyes/irises, voice patterns, and the like, behavioral characteristics are sometimes considered in tandem with biometric identifiers.

3. In traditional knowledge- or possession-based identification and authentication systems, disclosure of a subject's stored credential (e.g., a shared secret such as a password or a private certificate key) completely compromises their account's security. In contrast, biometric systems rely on measuring, storing, and comparing measurements derived from a person. The subjects and their features, not the measurements of them, are the credentials in a biometric system. These features are not easily changed, and because the subject remains a public person, some features cannot be presumed to be maintained in secrecy. Accounting for this reality, well-designed biometric systems emphasize process integrity as much as secrecy, to ensure that the chain of custody from sample capture, comparison, and returning results are protected from tampering or manipulation - even by an imposter armed with stolen or publicly-captured biometric data. The biometric data processes must be cryptographically protected so that tampering would be readily apparent.

4. The existing lack of clarity is exacerbated by the rapid development of biometric technology, as developers continue to modify existing technology and develop new ways to verify and/or identify individuals based on biological, physical, and behavioral characteristics. The rise of passive and/or dual authentication using both biometric information and behavioral characteristics is one example of a development in technology that was not anticipated at the time the first of the existing biometric statutes was enacted.

5. Legal definitions vary across jurisdictions and have raised significant disputes over the appropriate scope and correct interpretation of these laws. As but one example, there is ongoing litigation under the Illinois' Biometric Information Privacy Act (BIPA), as to whether a faceprint derived from a publicly-available photograph is a biometric identifier. A challenge for any proposed law will be to remain applicable with future advances in biometrics.

6. A heated policy and legal debate has emerged over whether biometric identifiers raise distinctive risks, and whether an individual has an inherent or even Constitutional right to privacy that would encompass that person's biometric information. This debate weighs individual rights to privacy against, for example, the rights of an entity to mitigate risks of proxy fraud or double dipping, which is one of the oldest and best use cases for biometrics.

C. General Features of Biometric Identification and Verification Systems

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

(a) Verification, or 1:1 matching, compares an existing template of the biometric identifier to a newly acquired template in order to verify a person's identity, for example unlocking a mobile phone using a fingerprint or face template.

(b) Identification, or 1:n matching, compares a newly acquired biometric template to a database of stored templates in order to identify an unknown person. Sometimes identification is used to streamline access to systems, allowing one touch access to electronic medical records and pharmaceutical cabinets in healthcare. By far, the most common use of identification search is to prevent and detect alias or duplicate enrollments, whether accidental or intentional, called "scrubbing" for double identity holders. Identification is also used by law enforcement and for background checks to search for matches against FBI criminal databases as part of character and fitness for bar membership, fiduciary licensure, and to check volunteers who will work with children under the PROTECT ACT, among others. Law enforcement facial recognition systems employ 1:n (and n:n) matching in public spaces to assist in identifying potential criminal suspects. Use of facial recognition technology to prevent and respond to criminal threats is also being used by private entities, such as retailers.

2. Most of these types of biometric systems follow a basic operating model that includes the following components:³

(a) *Acquisition and Enrollment*: a digital system captures a raw data sample of a particular physical feature from an individual. Some biometrics, like fingerprints, typically require direct contact with a device, capturing a 2D image of the friction ridges present on the subject's finger pad. Others, such as facial recognition, can be acquired from a distance or using existing other sources, such as government ID or even social media postings and other publicly-available photographs. Behavioral biometrics capture rich motion sensor and touchscreen data from a subject's phone, mouse movements, or keyboard activity from a desktop.

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

³ This description is adapted from Andrew Rice and Isabelle Moeller eds., *United Nations Compendium of Recommended Practices For the Responsible Use & Sharing of Biometrics in Counter Terrorism Final Draft* (June 2018) at 10-11, available at https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf.

(b) *Data Extraction*: the system then uses an algorithm to convert the raw sample into a digital biometric template recording the unique landmarks derived from the subject's sample. This enables the system to associate that template with an identifier, and then to store it either in a database of templates or in a record of information on the subject. In some cases, such as a digital eID, the record is placed on a phone or smartcard and is carried by the subject.

(c) *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.

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

(e) *Data Matching*: systems use a computer algorithm to determine whether the new template matches an existing template(s) from the database or a personally-carried medium.

(f) *System Parameters*: most systems allow the end-user/operator to define the parameters for when a new sample potentially "matches" the existing record or records.

IV. APPLICATIONS AND PRIVACY HARMS/ISSUES

A. Benefits of Biometrics

1. Reliability of identification

- (a) Immutability of biometrics and reliability of identification
- (b) Stability of biometrics over time
- (c) Cannot be transferred or shared – e.g., biometric timeclocks prevent "buddy punching," medical benefits can be secure
- (d) Strongly bound to an individual – difficult to shed a past identity, and can detect duplicate and alias identities

2. Security

- (a) Difficult to falsify/protects against identity theft
- (b) Prevent improper access (e.g., workstations, ATMs)
- (c) Prevent account takeovers (phishing) and handovers (unauthorized delegation)

3. Efficiency in Use

(a) Very fast verification – e.g., using a quick fingerprint scan versus entering a username and password

(b) Mitigates human errors – e.g., lost access cards, forgotten passwords or PINs, etc.

(c) Cost-effective – place scanners at access points vs. provide each and every person with a card or token they may lose

4. Personal Empowerment

(a) Allows individuals to make personal health and lifestyle choices

(b) Provides data to individuals for their own knowledge and application

(c) Can tailor experience to consumers based on physical needs

B. Risks of Biometrics

1. Exposure to data breaches/hacking

(a) Because the physical features measured by biometrics are cannot be changed like a password or social security number, the integrity and security of biometric systems is paramount to prevent unauthorized access to or substitution of data and to cryptographically detect tampering or manipulation by introducing stolen biometric samples into a high-stakes biometric authentication.

(b) Biometrics can be used to identify individuals without additional information, unlike other immutable characteristics such as DOB which cannot identify a specific individual without more information.

(c) Legacy software systems; lack of due diligence in assuring integrity and security.

2. Disclosure and data sharing/long-term storage

(a) Who owns/controls the data?

(b) Change in use of data with subsequent holders of data

(c) Function creep/immutable identifiers and the risk posed by future technological development

3. Tracking

(a) Individual/mass surveillance

(b) Location tracking without user's knowledge

- (c) Behavioral tracking without user's knowledge
- (d) Social engineering

4. Accuracy

- (a) False positives – e.g., facial recognition in law enforcement
- (b) False negatives – e.g., techniques of occlusion or confusion cause facial recognition failure
- (c) Impact of external factors – e.g., injury, weather, physical changes, etc.

5. Bias and discrimination

- (a) Accuracy – biometric technology often relies on partial information to authenticate identity (e.g., matching scans may measure only a small subset of points to confirm a match)
- (b) Inequitable deployment
- (c) Disability discrimination
- (d) Standardization/interoperability magnify security risks

6. Bioethical Considerations

(a) The use of biometrics has ethical implications, which overlap with and inform analyses in considering the regulation and implementation of biometrics. Bioethical considerations include various privacy interests, function creep (i.e., the use of biometric information beyond the purpose for which it was collected), individual autonomy (control over identifying information), discrimination, and dangers inherent in the commodification or informatization of the human body (or data about that body).

(b) In addition to issues raised by so-called first-generation biometrics (concerned mostly with identification), more recent analysis has focused on “behavioral biometrics” aimed at predicting a person’s behavior or intentions and branding (identifying) humans for the purpose of social control.

(c) The general concern of bioethics and “the dignity of embodiment” may help discussions surrounding new biometric technologies. Some authors are concerned that the pursuit of profit and pleasure can degrade human dignity, thus raising the need for a countervailing effort and regulation.

(d) These issues implicate competing frameworks of utilitarian policymaking as opposed to rights- or autonomy-based considerations.

7. Hygiene

(a) Epidemiological protocols should be considered in connection with the use of technologies using point of contact – e.g., finger scans.

C. Balancing Interests/Trade-offs and Application of Biometrics

1. Facial Recognition

(a) Facial recognition technologies (FRT) are one of the fastest growing biometric sectors and also perhaps the most controversial. Private entities use facial recognition technology in a variety of ways ranging from the photo-tagging technology involved in the Facebook litigation to device security for unlocking smartphones. These applications fall generally into five main categories: (1) safety and security; (2) access and authentication; (3) photograph and video storage identification and organization; (4) accessibility to platforms, accounts, or services; and (5) marketing and customer service.

(b) Law enforcement agencies typically use FRT systems either to verify a person's identity or identify an unknown person, often from a photo taken at a crime scene, by comparing a new image against an existing database of face templates and, more recently, using live FRT systems.⁴

(c) FRT systems illustrate many of the risks posed by biometric technologies.

2. Notice and Consent:

(a) Face images can be collected much more easily than other biometrics, like fingerprints. Indeed, the profusion of privately uploaded images on social media and other internet platforms and their use by private companies to train FRT algorithms is credited as one of the drivers in dramatic improvements in facial recognition technology while raising concerns over whether and how access to those images should be regulated.

(b) Even where user consent is obtained before collecting face images, the images often are redeployed and processed in an FRT system for a very different purpose. For example, many U.S. states have included face templates derived from drivers' license photographs in their FRT databases, often without any specific legal authorization or notice to the public. Some state and federal agencies also pay to access private FRT databases where the consent questions are even murkier.⁵

⁴ IJIS Institute, *Law Enforcement Facial Recognition Use Catalog* (2019).

⁵ A recent New York Times article describes the now-infamous example of Clearview AI's FRT system which has been used by federal and state law enforcement agencies. See Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times* (Jan. 18, 2020), at <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

3. Accuracy:

(a) The accuracy of an FRT system depends on multiple factors, including the quality of both the image used to create the template and the probe image used to conduct the search, the accuracy of the algorithm, the parameters used for the search, and the skill of the human examiner.⁶ NIST's ongoing evaluation of FRT algorithms recently concluded that the theoretical accuracy of these systems for 1:n identification have experienced "massive gains" between 2013 and 2017, but those results used relatively high quality images obtained in close-to-ideal settings.⁷

(b) The recent mis-identification of Robert Williams as a suspect in a robbery by Detroit police using the Michigan State facial recognition system illustrates these issues. According to media stories, the Detroit police used a low-resolution screen capture from a surveillance camera as the probe photo and the search returned Mr. Williams' photo as a potential match.⁸ Michigan uses the Rank One system, which has scored highly on the NIST FRVT tests, but those scores are based on relatively high quality photographs.⁹

4. Discrimination and Bias:

(a) A recent study by NIST concluded that most of the algorithms tested, with some notable exceptions, had higher error rates for some demographic groups for both verification and identification.¹⁰ Even where the underlying technology is highly accurate across demographics, however, the relative over-deployment of these systems in communities of color as well as the overrepresentation of racial minorities in law enforcement FRT databases raise independent problems of bias.

5. Mass Surveillance:

(a) The proliferation of high-resolution cameras in public and private spaces combined with the rapidly advancing capabilities of FRT systems gives law enforcement the ability to conduct real-time mass surveillance of particular events and, in urban areas, to retrospectively reconstruct people's movements

⁶ Patrick Grother, et al., *Facial Recognition Vendor Test (FRVT): Part 3: Demographic Effects*, NISTIR 8280 (2019), 15.

⁷ Patrick Grother, et al., *Facial Recognition Vendor Test (FRVT): Part 2: Identification*, NISTIR 8271 Draft Supplement (2020), 2-3.

⁸ Bobby Allyn, "'The Computer Got It Wrong:' How Facial Recognition Led to False Arrest of Black Man," NPR, June 24, 2020, available at <https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig>.

⁹ Pares Dave, "Face Recognition vendor vows new rules after wrongful arrest in U.S. using its technology," Reuters, June 24, 2020, available at <https://www.reuters.com/article/us-michigan-facial-recognition/u-s-activists-fault-face-recognition-in-wrongful-arrest-for-first-time-idUSKBN23V1KJ>; <https://www.rankone.io/> (citing NIST FRVT results).

¹⁰ <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>.

using recorded video. These new capabilities both intensify the privacy risks posed by the technology and raise new concerns that the prospect of live surveillance could chill freedom of speech and exacerbate the discriminatory effects of over-policing in poor and minority communities.

6. Schools

(a) Biometric technology employed in education can enhance school safety as well as streamline certain school administrative functions. Regarding safety, facial recognition systems can determine whether an “outsider” or a “flagged individual” has entered a school campus, such that the security system would send automatic notifications to school security staff and/or law enforcement.

(b) K-12 schools can require student fingerprint scans for both arrival and departure, with automatic alerts sent to parents regarding the whereabouts of their minor children.

(c) Many school systems in the US already use fingerprint biometrics to automate payments for school lunches, allowing students on free and reduced lunch to be indistinguishable from students paying on cash account.¹¹ Before biometrics, teachers had to distribute ID cards before lunch and then collect them after lunch so they are not lost.

(d) Schools use fingerprint scans to automate access to libraries preventing student ID card sharing to bring non-students into the library¹².

(e) Higher education institutions can use biometrics to grant students and faculty entry into various campus buildings and to proceed through campus security checkpoints.

(f) Regarding streamlined administrative functions, fingerprint scanning could replace conventional attendance-taking, making truancy easier to track.

(g) The Family Educational Rights and Privacy Act of 1974 (FERPA) already protects the disclosure of PII in educational records, including biometric identifies. *See* 34 C.F.R. § 99.3. However, parents and adult students may be able to launch a due process challenging the collection and use of biometric markers as a condition for education under *Goss v. Lopez*, 419 U.S. 565, 574 (1975), which held that, while “[t]he authority possessed by the State to prescribe and enforce standards of conduct in its schools . . . [is] concededly very broad . . . the State is constrained to recognize a student’s legitimate entitlement to a public

¹¹ For example, https://journalstar.com/news/local/education/some-lps-students-scanning-fingers-to-get-their-school-lunch/article_122d8ce3-8dbe-5f03-9f71-eb3432db31b6.html

¹² For example, <https://blog.library.gsu.edu/2016/11/03/registration-begins-for-new-bioscanners-at-library-entrances/>

education as a property interest which is protected by the Due Process Clause. . . .”

(h) Of course, educational institutions employing biometric data for student tracking and safety would also have to institute sufficient security measures to prevent the accidental disclosure of such data and to prevent breach of their data systems.

7. Employment

(a) Biometric technology is utilized in employment settings as a way of tracking time and attendance of employees. In addition to simplifying and streamlining employee tracking, requiring employees to punch in and out using a finger or palm scan allows for more accuracy in tracking time records and minimizes “buddy punching.”

(b) Employers might require the use of biometric timekeeping as a condition of employment (which Illinois’ BIPA expressly allows). Mandating the use of a biometric timekeeping system as a condition of employment could be viewed as in tension with an emphasis on consent as a requirement for data collection.

(c) Employees scanning their fingers or palms have noticed that their biometric information is being collected and compared to live scans every day.

(d) The reasonable expectation for any employee in using a biometric timekeeping system is that the use and retention of the data will be limited to the time and attendance system utilized by the employer. The question is not whether the data is “disclosed” to others within the time and attendance process (such as the timekeeping system provider or a cloud-based third-party data storage), but rather whether the data is disclosed to any third party for some use other than in connection with the time and attendance system.

8. Airport Security

(a) In U.S. airports, voluntary systems for streamlining passenger identification have been very successful. CLEAR ID is a privately-operated TSA-sanctioned trusted traveler program which allows travelers who submit to a background screen, enroll their fingerprint plus iris biometrics, and pay a fee, to bypass the security lines after verifying their biometrics at special CLEAR ID kiosks.

(b) Before COVID-19, CLEAR ID had expanded their venues to include Hertz Rental Car Fast Lane automated check-out, and was deployed at many sports stadiums around the country for streamlined entry to events. Delta, as one of the first partners of CLEAR, took an ownership stake in the company, and allowed Sky Club members to use CLEAR for free to streamline club access.

(c) In contrast, in 2018 and 2019, Customs and Border Patrol (CBP) and Delta, as well as several other airlines, deployed a curb-to-gate facial recognition system for international gate departures,¹³ intending to automate the repetitive manual identity verification process required by CBP to confirm a passenger at each stage is the same individual whose passport was used to book the flight.

(d) Unlike CLEAR ID, this was not a voluntary opt-in program, though it did offer passengers the opportunity to opt out and be verified manually.

(e) Privacy advocates voiced concerns about the use of the technology based on claimed facial accuracy questions, despite the fact that the system offered human verification alternatives, and relied on matching anonymized face scans against manifest documents including stored passport photos and other information already retained by CBP.

V. EXISTING LAWS AND PRINCIPLES

A. Overview

1. Three states – Illinois, Washington, and Texas – have enacted statutes that specifically address biometric privacy; the Illinois law alone provides a private right of action for state residents. Biometric information is separately regulated by some other states' consumer privacy statutes, including the California Consumer Privacy Act (CCPA). Many states have also amended their data protection and breach notification laws to include biometric information.

2. Beyond these, a number of proposed federal and state biometric privacy laws have been introduced, and industry groups and privacy organizations have published guidelines and standards. In addition, several consumer protection claims brought by Vermont's attorney general against a company that collects and uses consumer biometric information survived a motion to dismiss. Industry regulations may also apply to companies that collect biometric data.

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

4. Government acquisition and use of biometric information is governed broadly by the U.S. Constitution and, at the state and local levels, a growing number of ordinances regulate the acquisition of surveillance technologies and, more recently, ban the use of facial recognition.

5. The below is a sampling of some approaches existing and proposed laws and frameworks use to regulate biometric information and systems that the drafting group should

¹³ See, e.g., <https://news.delta.com/sites/default/files/ig%200927ATL%20F%20biometrics%20how%20it%20works.pdf>.

consider as part of its analysis. It is not comprehensive, but provides a representative sample of major laws and policy recommendations with a focus on U.S. materials, organized by issue.

B. U.S. Consumer Biometric Privacy Laws

1. Biometric/Covered Information Definition

(a) The two other state consumer biometric privacy statutes, and the proposed 2020 National Biometric Information Privacy Act (NBIPA),¹⁴ follow the Illinois BIPA model and define biometric data as digital representations of physical traits that have been processed into a digital representation or template for computer processing. These definitions typically include a long list of “biometric identifiers” that are commonly used for identification and/or verification, along with a list of specific exceptions and define “biometric information” broadly as any information based on one of the listed identifiers used to identify an individual.

(b) The rapidly evolving nature of biometric technology and the challenges defining the term “biometric” have led to significant legal disputes under IL BIPA, including how to apply the definition to newer technologies and the scope of the exceptions, especially photographs. Recent litigation over Facebook’s face recognition and scanning technology, which the company claimed did not rely on facial geometry as required under IL BIPA, illustrates these challenges.¹⁵

(c) The CCPA offers an alternative model. It defines biometric information broadly based on the ability to extract an identifier template and also explicitly extends to keystroke and gait patterns as well as “sleep, health or exercise data that contain identifying information.”¹⁶ This directly extends the law to a newer set of applications that use supposedly unique individual traits or behaviors that might not be covered under narrower definitions and also creates flexibility for the law to encompass future applications but also creates new sources of potential ambiguity that may make compliance more difficult and are likely to lead to legal disputes.

2. Exemptions

¹⁴ National Biometric Information Privacy Act S. ___, 116th Cong. 2d Sess. (2020), available at <https://www.merkley.senate.gov/imo/media/doc/20.08.04%20National%20Biometric%20Information%20Privacy%20Act.pdf>.

¹⁵ See, e.g., *In re Facebook Biometric Information Privacy Litigation*, 2018 WL 2197546 (N.D. Cal. 2018) (applying Illinois law): Dismissing defendant’s motion to dismiss and holding that dispute over whether the social media defendant’s face recognition and scanning practices met the statutory definition were factual questions for the jury to decide. Plaintiffs disputed Facebook’s claim that the software it used did not rely on facial geometry.

¹⁶ CCPA section 3(e) (“Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted . . .”).

(a) Biometric privacy laws usually 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. Most biometric privacy laws carve out from coverage uses that would otherwise be covered by these sector-specific laws.

(b) Biometric privacy laws also tend to make exceptions for uses that are pursuant to a valid warrant or subpoena. *See* 740 ILCS 14/15(d).

(c) IL BIPA exempts financial institutions or affiliates subject to GLBA; information captured from patients in a health care setting or HIPAA covered information; and contractors or agents working for the state or local government. 740 ILCS 14/25(b), (c). That law also clarifies that it should not be construed to impact the admission of biometrics in court or other proceedings. *Id.* at 14/25(a).

(d) The Washington law provides for GLBA and HIPAA exemptions, but also carves out uses “in furtherance of a security purpose” and a law enforcement officer acting within the scope of his or her authority. RCW 19.375.020(7), 19.375.040

(e) The exemptions in the Texas law are narrower, only carving out voiceprint data retained by a financial institution or an affiliate of a financial institution under GLBA from the application of the statute. § 503.001(e).

3. Scope

(a) Current laws and the NBIPA legislation apply broadly to most private entities but exclude public entities. Some critics of these laws have called for narrowing their scope. For example, in 2019, the Illinois Legislature rejected SB3053, which would have amended the scope of IL BIPA to exclude biometric information “used exclusively for employment, human resources, fraud prevention, or security purposes” if “the private entity does not sell, lease, trade, or similarly profit” from the information or “stores, transmits, and protects the biometric identifiers” in the same fashion and to the same degree as other confidential information.¹⁷

(b) Conversely, others have criticized the exclusion of public entities due to the ease with which government entities can obtain privately-collected biometric data, and the difficulty in clearly demarcating public and private activities.¹⁸

(c) A related issue is whether biometric information should be regulated under a separate statute or incorporated into existing comprehensive

¹⁷ IL SB3053 (2019), at <https://legiscan.com/IL/text/SB3053/id/1731625>.

¹⁸ *See, e.g.,* Amba Pak ed., *Regulating Biometrics: Global Approaches and Urgent Questions* (September 2020).

consumer privacy laws. CCPA and the COPRA legislation are examples of an integrated approach.

4. No Sale/Disclosure

(a) As described earlier, the immutable nature of biometrics heightens the risks associated with their disclosure to third parties. Current and proposed laws deal with this by prohibiting the sale or profit from biometrics and/or placing restrictions on their disclosure.

(b) IL BIPA and the NBIPA prohibit sales or other profiting from a person's biometrics even where there is adequate notice and consent. 740 ILCS 14/15(c) (no sale, lease, trade, or other profiting); NBIPA § 3(c) (same but includes "use for advertising purposes" among prohibited activities). This is a different approach than is taken by the CCPA, which regulates biometrics as personal information. That statute permits businesses to sell personal information (with "sell" being broadly defined to include any transfer or disclosure for value), but they must provide individuals with a right to opt out.

(c) The consumer biometric privacy laws also place restrictions more generally on the disclosure of biometrics, permitting disclosure only where there is notice and consent; where the disclosure is necessary to provide a product or service explicitly requested by the individual; or to effectuate a financial transaction. Allowances are also made for where the disclosure is required by law or made pursuant to a warrant or subpoena. For example, NBIPA permits disclosure but only where the individual provides a written release "immediately prior" to that disclosure. NBIPA § 3(d)(1). A written release is not required where the disclosure or redisclosure completes a financial transaction requested or authorized by the individual, or where it is required by law or pursuant to a valid warrant or subpoena. NBIPA §§ 3(d)(2), (3).

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

(e) These approaches raise the question of whether it is desirable as a policy matter to prohibit sales of or profiting from biometric disclosures, including in instances where an individual is making an informed choice about the disposition of their own biometric information as discussed in further detail below. They also raise the question about whether the desirable policy scheme would involve a right notice/informed consent before disclosure or a right to opt out, potentially afterwards, with the attendant questions of whether biometric disclosures, or the related consent, can be rescinded effectively. In addition, there is also the question of whether it makes sense to write service provider exceptions

into the law, and under what circumstances, and whether individuals can sell or profit off of their own biometric disclosures.

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

5. Notice/Consent

(a) 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.

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

(c) The CCPA permits businesses to sell personal information, including biometric information, but requires notice and a right to opt out. An opt-out gives consumers the ability to direct a business not to sell their personal information, including biometric information, to a third party, but does not stop a business from distributing the data within the organization that collected it (even to different business units). Businesses who receive a request to opt out must stop selling personal information (with some exceptions) and may only request that an individual opt back in after 12 months. There are some timing questions about how the notice and opt-out provisions apply and whether there may be a gap between when an individual requests an opt-out and when the business ceases selling the information.

(d) The Washington law requires a “context-dependent” disclosure given “through a procedure reasonably designed to be readily available to affected individuals” prior to enrolling a biometric in a database. RCW 19.375.020(2). The law specifies that the “exact notice and type of consent required to achieve compliance with subsection (1) of this section is context-dependent,” but is something less than affirmative consent. *Id.* 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.” *Id.* at § 5.

(e) The FTC advocates a similar approach in its 2012 Staff Report, “Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies,” which includes as a best practice providing clear notice to individuals prior to any use of facial recognition technology. The FTC also advocates for affirmative express consent prior to any use that is materially different than what was represented to the individual at collection. The FTC approach differs from the existing biometric privacy laws, however, in that it

explicitly gives individuals the right to opt out of the use of their biometrics, whereas the consumer biometric privacy laws do not tend to provide individuals with a clear right to opt out of the use of the technology.

(f) NBIPA addresses concerns about potential coercion and lack of choice by requiring “written release,” and defining that term to mean “specific, discrete, freely given, unambiguous, and informed written consent given by an individual who is not under any duress or undue influence of an entity or third party at the time such consent is given.” NBIPA § 2(4). The proposed legislation also specifies that a written release cannot be sought as part of, or combined with any other consent or permission and that it may not be combined with an employment contract. *Id.* at § 3(b)(2).

(g) The difference between notice and consent is meaningful here and may be exacerbated by different proposed and actual regimes: for example, a broad notice that informs consumers that their biometric information may be used by multiple or unlimited third parties without a right to give or withdraw consent is meaningfully different from one that seeks and gets informed consent for use by each third party or on or before when sale or disclosure may be made. Opt-outs with time limitations on opting back in may also address questions of ongoing use, but raise questions of retroactivity.

(h) The Washington law also permits disclosures for service providers or where a third party contractually promises not to further disclose the biometrics without notice and consent.

6. Retention

(a) Risks relating to the retention of biometrics include that they, unlike alphanumeric credentials, maintain their value as identifiers. In addition, storage for longer than needed increases the risk of data theft, that consent will no longer be informed and valid, or that the uses are consistent with the purposes of the original collection.

(b) IL BIPA and NBIPA require the creation of a retention schedule and guidelines for destroying biometrics, both of which must be publicly available. For example, NBIPA requires that entities need to “develop and make available to the public a written policy establishing a retention schedule and guidelines for permanently destroying” biometrics. NBIPA § 3(a)(1).

(c) The consumer biometric laws also generally impose an upper limit on the retention period, pegged to the purposes or services for which the biometrics were collected. The IL BIPA allows for retention until the “initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of the individual's last interaction with the private entity, whichever occurs first.” 740 ILCS 14/15(a). The Texas law requires retention within a “reasonable period of time” but then caps that period at a year

after there is no longer a valid reason for maintaining the biometric. Tex. Bus. & Com. Code Ann. § 503.001(c)(3). Where the biometric serves the purpose of employee identification (“security purposes”), then the biometric must be destroyed within a year after the employment relationship is terminated. *Id.* at § 503.001(c)(3)(c-2). NBIPA requires destruction not later than when “the initial purpose for collecting or obtaining” the biometrics has been satisfied or “1 year after the individual’s last intentional interaction with the private entity.” NBIPA §§ 3(a)(1)(A), (B). The FTC in its Staff Report includes as a best practice establishing and maintaining “appropriate retention and disposal practices for the consumer images and biometric data.”

(d) Considerations 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.

7. Enforcement/Penalties

(a) As detailed above, numerous harms can follow from the improper use or disclosure of biometrics. Existing laws provide recourse for individuals, serving the dual purposes of loss recovery and deterrence.

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

(c) The IL BIPA provides a private right of action. 740 ILCS § 14/20. Current Illinois caselaw allows for standing even where there is merely a statutory violation; a showing of harm is not a requirement. NBIPA takes a similar approach by providing a private right of action, and clarifying that a violation constitutes “an injury-in-fact and a harm.” NBIPA § 4(a) & (c).

(d) The NBIPA also permits enforcement by a state attorney general. NBIPA § 4(b). The Texas law is only enforceable by the state attorney general. § 503.001(d). The Washington law is enforceable by the state attorney general as an unfair or deceptive act and/or unfair method of competition. RCW § 19.375.030(2).

(e) There has been an enormous number of class action suits filed under the IL BIPA, especially in light of recent court decisions holding that private litigants have standing for procedural violations of the statute. This raises the question of whether state attorneys general should be solely vested with enforcement authority where they do not appear to be actively pursuing investigations, leaving individuals without any other recourse.

(f) Each of the biometric privacy laws provides for monetary penalties and other compensation, as follows:

(i) NBIPA

- a. Negligent violation: greater of \$1,000/per violation or actual damages. NBIPA § 4(e)(1)(A)(i)(I)(II).
- b. Intentional/reckless violation: “sum of” actual damages and punitive damages up to \$5,000/violation. NBIPA § 4(e)(1)(A)(ii)(I)(II).
- c. Reasonable attorneys’ fees and costs, including expert witness fees and other litigation expenses. NBIPA § 4(e)(1)(B).
- d. Injunctive or other appropriate relief. NBIPA § 4(e)(1)(C).
- e. Specific performance of destruction requirement. NBIPA § 4(e)(2).

(ii) IL BIPA

- a. Negligent violation: greater of liquidated damages of \$1,000 or actual damages. 740 ILCS 14/20(1).
- b. Intentional/reckless violation: greater of liquidated damages of \$5,000 or actual damages. 740 ILCS 14/20(2).
- c. Reasonable attorneys’ fees and costs. 740 ILCS 14/20(3).
- d. Other appropriate relief, including an injunction. 740 ILCS 14/20(4).

(iii) Washington

- a. Not more than \$2,000 per violation. RCW § 19.375.030(2); RCW § 19.86.140.

(iv) Texas

- a. Civil penalty of not more than \$25,000 per violation. § 503.001(d).

8. Security.

- (a) As sensitive, personally-identifying data, biometrics pose significant data security risks, including the possibility of a data breach either caused by hacking, human error, or inadvertent disclosure, to name a few. There

are also risks where biometrics are transferred to new systems, either where a company is upgrading its technology or through a merger and acquisition.

(b) The current and proposed biometric privacy laws approach data security by providing a baseline standard for security. For example, NBIPA requires 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.” NBIPA § 3(e). If NBIPA were enacted, this essentially would be the same standard as in IL BIPA and the Texas law, *see* 740 ILCS § 14/15(e) and § 503.001(c)(2), with the Washington law requiring only “reasonable care.” RCW § 19.375.020(4)(a).

(c) Providing a baseline standard is also the approach advocated by the FTC in its 2012 Staff Report, “Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies,” and is how the FTC has approached data security in its Section 5 orders until recently. Among the best practices that are highlighted in the report are that companies should maintain reasonable data security protections for consumers’ images and biometric information collected from those images to enable facial recognition. *Id.* at ii.

(d) General privacy laws that encompass biometrics also require a baseline level of security, with the CCPA permitting private rights of action where a data breach results from a business’ “violation of the duty to implement and maintain reasonable security procedures and practice appropriate to the nature of the information.” 1798.150.

(e) The general trend in data security laws is towards more specific requirements, though there is debate whether that approach is appropriate given the rapidly evolving security threat landscape. For example, the NY Shield Act,¹⁹ which includes “biometric information” in its definition of “private information” regulated under the statute, requires reasonable safeguards to protect the security, confidentiality, and integrity of private information, including its disposal. N.Y. Gen. Bus. Law § 899-bb(2)(a). Under the law, covered entities have reasonable safeguards either where they (1) are a compliant regulated entity under HIPAA, GLBA, or NY DFS Cybersecurity Regulations, or (2) implement a data security program that includes a number of enumerated administrative, technical, and physical safeguards and timely dispose of personal information after it is no longer needed. N.Y. Gen. Bus. Law § 899-bb(2)(b).

(f) The HIPAA Security Rule, which also regulates biometrics in certain contexts, also takes a more specific approach to outlining data security

¹⁹ Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), N.Y. Gen. Bus. Law § 899-bb.

requirements, though it is designed to be flexible and scalable given the diversity of the healthcare marketplace.

(g) Given the sensitive nature of biometrics and security risks, a relevant question for evaluating proposed legislation or frameworks will be whether establishing a baseline standard is advisable or whether something more should be imposed, for example a risk analysis and management requirement, as well as technical, administrative, and physical safeguards for the information. Although specific requirements are less flexible, they do lead to more certainty for businesses when designing their compliance programs and defending against enforcement actions.

(h) Consideration should also be given as to whether documented adherence to a recognized data security standard could constitute an affirmative defense to a tort claim. While this is typically the practical effect of having a data security program that aligns with established standards, this could be established as a safe harbor to liability, similar to the approach taken in Ohio. Ohio Rev. Code § 1354.01, et seq.

C. U.S. Sector Specific Privacy/Data Security Laws

1. HIPAA Privacy Rules

(a) Protected Health Information (PHI) is any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA-covered entity. PHI also includes biometric identifiers, including fingerprints and voiceprints. 45 C.F.R. 164.512.

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

(c) Key concepts and principles under HIPAA include ensuring a federal “floor” of privacy protection rather than a “ceiling,” which preempts any state laws that do not provide the same level of privacy protection as or are inconsistent with those federal protections. State laws with more stringent protections supersede HIPAA. HIPAA carves out the need to obtain individual consent or authorization for public health activities and public purposes established under state laws that prescribe exceptions or mandatory reporting such as for health oversight, law enforcement, organ or tissue donation, research, judicial proceedings, or when necessary to avert serious threat of harm to the individual or other persons. Otherwise, HIPAA allows for the use and disclosure of such for treatment, payment, or healthcare operations without written authorization as long as the CE provides written notice of their privacy practices that clearly describes among other things such uses and disclosures, their duties to and the rights of patients, and complaint procedures. Other uses and disclosures such as research, education, marketing, or fundraising may be carved out, or

permitted with or without written consent and authorization. For example, research may require either an IRB waiver or written consent. Marketing requires written authorization especially if the CE receives direct or indirect reimbursement from third parties, but it does include all communications that promote health-related products or services. Fundraising may require the opportunity to opt out. An individual also has the right to access or obtain copies of their PHI and obtain an accounting of disclosures made to unauthorized third parties. There is no private cause of action allowed to an individual to sue for a violation of the federal HIPAA or any of its regulations.

D. International/Non-U.S. Laws

1. GDPR

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

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

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

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

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

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

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

2. Other

(a) At the foremost edge of European thinking on the topic, some authors have begun discussing the possibility of drawing on the Roman law principles regarding *res extra commercium*, (things not tradeable/things beyond commerce). They argue that commerce in some data is, and should be, prohibited by the law because some data embody values and interests (e.g., personal dignity) that would be detrimentally affected by trade. They observe that transactions in personal data are not forbidden but subject to what they will call a dynamically limited alienability rule. This has potential implications for general contract laws as well. *See* Janeček, V., & Malgieri, G. (2020). Commerce in Data and the Dynamically Limited Alienability Rule. *German Law Journal*, 21(5), 924-943. doi:10.1017/glj.2020.47

(b) For a recent survey of (almost) all other privacy laws worldwide see Greenleaf, Graham, *Global Tables of Data Privacy Laws and Bills* (6th Ed. January 2019), Supplement to 157 Privacy Laws & Business International Report (PLBIR) 16 pages, Available at SSRN: <https://ssrn.com/abstract=3380794>. See also the references in Appendix A.

E. Public-Sector Facial Recognition Bans

1. A small but growing number of U.S. municipalities’ and counties’ jurisdictions have passed bans on the use of facial recognition technology by public entities and/or law enforcement. Advocates of these bans argue that facial recognition poses distinctive privacy risks over other information and biometric technologies and that law enforcement use typically lacks either express legal authorization or limitations.

2. Facial Recognition and Biometric Technology Moratorium Act of 2020, S.4084, 116th Cong. (2020): There have been several recent federal legislative proposals addressing facial recognition. This most recent bill:

(a) Prohibits the use of facial recognition technology by federal entities, which can only be lifted with an act of Congress;

(b) Prohibits the use of other biometric technologies, including voice recognition, gait recognition, and recognition of other immutable physical

characteristics, by federal entities, which can only be lifted with an act of Congress;

(c) Conditions federal grant funding to state and local entities, including law enforcement, on those entities enacting their own moratoria on the use of facial recognition and biometric technology;

(d) Prohibits the use of federal dollars for biometric surveillance systems;

(e) Prohibits the use of information collected via biometric technology in violation of the Act in any judicial proceedings;

(f) Includes a private right of action for individuals whose biometric data is used in violation of the Act and allows for enforcement by state Attorneys General; and

(g) Allows states and localities to enact their own laws regarding the use of facial recognition and biometric technologies.

F. Industry/Advocacy Group Principles

1. An increasing number of organizations, including trade groups, privacy advocacy groups and individual companies have published principles and best practices for biometric technologies, in particular for facial recognition technologies, which have come under increased scrutiny in recent years.²⁰

2. Most of these include some version of following general principles but with substantial variation in the details of how to implement them:

- Transparency/Notice
- Meaningful Consent
- Data Quality
- Validated Accuracy
- Non-Discrimination
- Data Security
- Accountability

²⁰ Examples include: Security Information Alliance, *Principles for the Responsible and Effective Use of Facial Recognition Technology*; IBIA, Future of Privacy Forum, *Privacy Principles for Facial Recognition Technology in Commercial Applications*; Fast Identity Online (FIDO) Alliance, *Privacy Principles*; World Economic Forum, *A Framework for Responsible Limits on Facial Recognition*.

- Privacy by Design

3. In addition to principles specific to biometric technologies, many groups have published recommendations for principles to govern the use of artificial intelligence in general, which would apply to most biometric technology systems. For example, NIST recently published for public comment the first draft of Four Principles of Explainable Artificial Intelligence (Draft NISTIR 8312), which recommends:

- AI systems should deliver accompanying evidence or reasons for all their outputs.
- Systems should provide explanations that are meaningful or understandable to individual users.
- The explanation correctly reflects the system’s process for generating the output.
- The system only operates under conditions for which it was designed or when the system reaches a sufficient confidence in its output. (The idea is that if a system has insufficient confidence in its decision, it should not supply a decision to the user.)

VI. RECOMMENDATIONS

A. Scope

Given the broad legal landscape addressing biometric privacy, the drafting group should consider a number of questions relating to the scope of any survey of existing laws/policies/principles. These include:

1. Should the drafting group focus only on consumer privacy laws or extend to laws relating to government applications?

- *We recommend that the drafting group focus on consumer biometric privacy laws but consider how those laws can or should limit access to this information by law enforcement or other government entities.*²¹

²¹ For example, on September 11, 2020, the Department of Homeland Security announced proposed rules regarding Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, which would require “that any applicant, petitioner, sponsor, beneficiary, or individual filing or associated with an immigration benefit or request, including United States citizens, must appear for biometrics collection without regard to age unless DHS waives or exempts the biometrics requirement.” The proposed rule would also “authorize biometric collection, without regard to age, upon arrest of an alien for purposes of processing, care, custody, and initiation of removal proceedings” as well as “define the term biometrics” and “increase the biometric modalities that DHS collects, to include iris image, palm print, and voice print.” The rule also “proposes that DHS may require, request, or accept DNA test results, which include a partial DNA profile, to prove the existence of a claimed genetic relationship and that DHS may use and store DNA test results for the relevant adjudications or to perform any other functions necessary for administering and enforcing immigration and naturalization laws.” See Federal Register Vol. 85, No. 177, at 56338 (Sept. 11, 2020), <https://www.govinfo.gov/content/pkg/FR-2020-09-11/pdf/2020-19145.pdf>.

2. Should the drafting group address sector-specific laws that might regulate biometrics in certain contexts?

- *We recommend that the drafting group consider: (a) the regulatory gaps that exist under the current legal structure in the U.S. and how to address those; and (b) whether specific aspects of sector-specific laws like HIPAA could be useful in addressing the risks we've identified.*²²

B. Questions for Consideration

The Brainstorming Group's analysis has distilled a number of legal and policy considerations that could be addressed by a drafting group. In particular, we recommend that the drafting group consider all or a subset of the following questions:

1. Structure: What is the best way to regulate the collection, use, and disclosure of biometrics? Is it through a standalone biometric privacy law or is it better integrated into general consumer privacy laws and regulated along with other types of (sensitive) personal information? CCPA, GDPR, and COPRA are examples of an integrated approach. BIPA and its state and federal variants illustrate the standalone approach.

(a) Is it feasible for one statute to cover all categories of data and use cases, especially where there are categories of data that are used for different purposes?

(b) Is it better to structure the law in terms of the type of biometric information at issue, the type of entity being regulated, the relationship between the entity and the data subject, or how the data will be used?

(c) A related question that the group could consider is whether to recommend a uniform federal law or a mix of federal and state regulation.

2. Scope of Coverage: What entities and which activities should the law cover?

(a) Should the law distinguish between or exempt certain activities? E.g., financial fraud, health care, or others?

²² For example, HIPAA creates a federal "floor" of privacy protection, preempting any state laws that do not provide the same level of privacy protection as or are inconsistent with those federal protections. It balances the rights of individuals to maintain the privacy of their health information with the needs of the healthcare covered entity to utilize that information for specific purposes (treatment, payment, and other healthcare operations) by requiring written consent for certain types of marketing, fundraising and research, and written authorization for any other access, use, or disclosure by or to third parties. However, HIPAA has not updated the advances in biometric technology, potentially excluding protections. And what may be for political expediency reasons, COPPA carves out HIPAA assuming it establishes sufficient protections to individuals in the healthcare sector.

(b) Should the laws apply equally to commercial entities as well as governments?

(c) What, if any, restrictions or requirements should be implemented in relation to government access to information collected by commercial entities?

(d) If the laws do not restrict government access, how should they address legal obligations to disclose biometric information in response to law enforcement requests or in the course of civil litigation?

(e) How should gaps in coverage be addressed? Some of the existing laws carve out entities covered by HIPAA to address healthcare data, creating gaps in regulatory oversight on entities collecting this type of information, since not all entities are covered under HIPAA. The same challenge applies with other federal statutes that only apply to certain entities or sectors. Exemptions in the law should take into consideration whether they are inadvertently statutorily deregulating certain types of categories of biometric data under the assumption that it is covered by another statute.

3. Biometric Definition: What aspects of biometric information should the law seek to protect?

(a) Should biometric privacy laws focus on biometrics used for identification/verification or extend to other categories such as health and genetic information or even any data related to biological activity?

(b) What specific categories of biometric information/activities should the law protect?

(c) How can the law address new technologies? Should the law attempt to anticipate privacy concerns raised by new biometric applications and technologies? Relatedly, should the law anticipate that innovation will enable additional types of data to function as biometric identifiers?

(d) Should biometric privacy laws exempt some activities and what are the criteria for exemption?

(e) How could the law ensure that the data is not repurposed for non-exempt activities?

4. Consent/Notice: What are some of the limitations of a notice/consent-based model and should certain uses be restricted and/or more heavily regulated?

(a) How should the law ensure meaningful consent and should there be different standards for different situations? For example, can an employee meaningfully consent to providing a biometric identifier where doing so is a condition of employment? What about consumer contracts where consent to

biometric data sharing or sale is one part of a larger consumer decision or added to updated EULAs?

(b) What obligations should transferors of biometric information have to obtain meaningful consent for subsequent use/sale/custody of biometric information? What about transferees?

(c) Should an effective notice and consent regime require consent before any use, sale, or transfer of biometric identifiers, or implement an opt out regime? How do each of these regimes address questions of subsequent use and retroactivity? Would they most effectively be combined?

(d) Should consent be revocable? If so, under what circumstances and what should the procedure be?

(e) How should consent requirements address the problem of mission creep?

(f) What limits, if any, should the law put on consent?

(i) Is a consent-based model sufficient to address all issues/appropriate for all contexts? Does this vary based on the model used (e.g., prior consent vs. opt out vs. licensure)?

(ii) Should certain uses be prohibited as a matter of public policy? For example, for minors? in contracts of adhesion? after a certain period of time? for certain kinds of biometric information?

(iii) What minimum protections should the law require even where consent is obtained?

(iv) Should consent expire? What about for minors? In specific contexts?

(v) Should there be limits on repeated attempts to gain consent when it is declined?

(g) What limits, if any, should a consumer biometric privacy law place on the obligation to provide biometric data to law enforcement? What about other government contexts (immigration, for example)? What about civil enforcement or subpoenas?

(h) What should the law require for effective notice?

(i) Should that requirement vary based on the context of the notice/sale/transfer?

(ii) Who should provide notice and what aspects of collection/processing/use should the notice include?

(i) Should the law prescribe standards for how notice is provided?

(j) Should there be a penalty for failure to provide notice independent of any other penalty or private right of action predicated on illegal sale or misuse of biometric information?

(k) What obligations should transferors of biometric information have to provide notice of subsequent use/sale/custody of biometric information? What about transferees?

(l) This section should be discussed in conjunction with the larger discussion of enforcement and penalties below.

5. Proportionality/Necessity: Should the law incorporate principles of proportionality and necessity for the collection and use of biometric data?

(a) For example, any processing of personal information under the GDPR must be both necessary (be effective and least intrusive) and proportionate (importance of the processing balanced against its intrusiveness).

(b) The FTC in its Facial Recognition Staff Report includes as a best practice that there be consideration given to the “sensitivity of information when developing facial recognition products and services.”

6. Enforcement/Remedies:

(a) Should the law be enforceable by private litigants, government regulators, or both?

(b) If the law authorizes a private right of action, should it prohibit consumer arbitration and/or class action waivers (either entirely, or in specified contexts) or should this be left to the contracting parties?

(c) Should violations of the law be enforceable under other applicable consumer protection laws or should the law preempt (all or conflicting) private remedies?

(d) Should the law prohibit the parties from contracting around the statutory requirements as a matter of public policy or provide that the available remedies are intended to supplement any applicable remedies for breach of contract?

(e) If the law authorizes government enforcement, which regulators should be responsible? The FTC, state attorneys general, sector specific regulators, or a new privacy or biometric regulator? Should there be dual

jurisdiction, as is the case with statutes like COPPA? What about criminal enforcement?

- (f) For each enforcement mechanism chosen:
 - (i) What standard of culpability should apply (strict liability, negligence, recklessness, or intentional conduct)?
 - (ii) Where a legal duty is required, should the statutory violation suffice to establish the duty?
 - (iii) Should a statutory violation be sufficient to establish liability and/or permit recovery or must there be an additional showing of harm?
 - (iv) Should the law include an opportunity to remedy a violation by, for example, obtaining consent or deleting the information?
 - (v) Should the available remedies vary depending on the statutory obligation violated?
 - (vi) Are there statutory provisions that should not be enforceable such as failure to provide required notices, obtain mandated consent for certain actions, follow opt out regimes, or comply with deletion requirements?
 - (vii) What remedies should be available for each violation: civil fines, officer/director liability, restitution, disgorgement, actual damages, statutory damages, nominal/exemplary damages?
 - (viii) Should private litigants be permitted to recover civil penalties for disbursement to the government?

7. Ownership vs. Data Custodian:

(a) Should laws and regulations treat data as owned by an entity or just regulate custodians of the data at every level? If applying an ownership model, should laws and regulations consider who “owns” the data and what rights does the owner have? Consider whether regulation should just cover any entity that touches the data, rather than ascribing ownership, which results in a licensing and sale model of information.

8. Accuracy/Fairness/Bias: Should biometrics laws address concerns about accuracy, fairness, and bias?

(a) Can and how should the law address more systemic issues that may arise with biometric technologies? For example, the problem of over deployment in marginalized communities.

(b) Should the law incorporate technical standards/frameworks to improve accuracy and fairness? Alternatively could the law prescribe a general standard to accommodate changes in technology and provide flexibility drawing on models from cybersecurity.

(c) Should the law incorporate general principles from AI ethics, including transparency, human involvement, and others, to mitigate algorithmic bias?

9. Data Security: Should the law address data security and, if so, to what extent?

(a) The current biometric privacy laws (state and NBIPA) approach data security by establishing a baseline level of security (“reasonable”) that provides companies with some flexibility in how they implement appropriate information security programs. Is this the correct approach given the sensitive and immutable nature of biometrics, or should there be specific administrative, technical, and physical safeguards required by law?

(b) Should documented adherence to third-party technical data security standards provide companies some level of protection against alleged violations of any security requirements in the law?

(c) Should there be some weighing of the costs of protections against the risk of harm (for example, a documented risk assessment process that would enable a company to identify and evaluate its risk tolerance)?

(d) Should the level of security required depend on the nature of the risk?

(e) Many of the state data breach laws include a “risk trigger” – i.e., notification is only required where there is a risk of harm to the individual from the disclosure. Should this concept be incorporated into the law, for example, by requiring a risk of harm before an individual can establish a violation of any security provision in the law?