

The Sedona Conference Draft Commentary on Notice and Consent Principles for Facial Recognition Technology (October 2021)



This confidential draft of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to comments@sedonaconference.org no later than November 29, 2021.

The Sedona Conference Draft Commentary on Notice and Consent Principles for Facial Recognition Technology (October 2021)

Drafting Team Members:

Arianna Evers (Drafting Team Leader)

Alexander Altman

Kate Baxter-Kauf

Sheryl Falk

Michael LeDesma

Melinda McLellan

Tom McMasters

David Mindell

Meredith Schultz

Hon. Gail Andler (ret.) (Judicial Advisor)

Starr Drum (Steering Committee Liaison)

Ruth Promislow (Steering Committee Liaison)

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. HOW FACIAL RECOGNITION TECHNOLOGY WORKS	3
III. USES OF FACIAL RECOGNITION TECHNOLOGY	6
IV. CURRENT U.S. APPROACH TO REGULATING FACIAL RECOGNITION TECHNOLOGY	8
V. RISKS OF FACIAL RECOGNITION TECHNOLOGY	12
A. Risks to Individuals	12
B. Challenges to Businesses	15
VI. EXISTING PRINCIPLES AND BEST PRACTICES	18
VII. PRINCIPLES	21
A. The use of facial recognition technology may pose unique privacy concerns, especially in the context of public sector use	21
1. Public sector actors may not be similarly situated to private actors in many of their actions, positions, and coercive power.	22
2. The relevant question for many governmental uses of facial recognition technology may not be based on the adequacy of notice and consent.	22
3. Notice and consent may not be an appropriate regime when the individual does not have control over the situation in some manner.	23
4. A notice and consent regime may be appropriate for government uses of facial recognition technology in certain circumstances, such as where the government is acting in a manner analogous to a commercial entity, and the use does not implicate constitutional concerns or collective autonomy.....	24
B. Actual notice should be meaningful and transparent.....	26
C. Individual consent for the use of facial recognition technology should be obtained wherever possible	27
1. Adequate consent may vary by stage.....	28
2. Adequate consent may vary by use.....	30
3. Secondary use and transfer may require heightened consent	31
4. Consent should be freely given and free from undue coercion or deception.	32

5.	Consent should be freely revocable.	33
D.	Where providing notice and obtaining consent are not feasible, entities must take measures to ensure accountable use of facial recognition technology.....	36
E.	Face geometry data should be subject to data security standards appropriate to the risk.....	41

I. INTRODUCTION

The recent development of sophisticated facial recognition software has generated unique opportunities for public and private sector application of the technology. As facial recognition software improves and image databases become larger and cloud-based, public and private sector entities are increasingly relying on the technology for various purposes, including law enforcement, security, and marketing. The technology offers many benefits, including making identification and verification of individuals more efficient. However, depending on the circumstance, the use of the technology has the potential to raise privacy, consumer protection, and civil liberties concerns in ways that other biometric technologies might not.

Despite its potential to affect our everyday lives and the unique risks posed by this technology, there is currently no uniform statutory or regulatory regime regarding its use in the United States. Although there are some federal privacy laws that are applicable to the use of facial recognition technology depending on the circumstance, there is no comprehensive federal privacy law tailored to the particular concerns arising from its use. This landscape, coupled with concerns expressed by some over the use of this technology in potentially problematic ways and without adequate safeguards, has led states and localities to regulate the technology themselves. In some instances, they have passed laws that attempt to impose boundaries and rules for how public and private sector entities can use the technology. In others, the reaction has been to impose moratoriums or outright bans on the use of facial recognition technology, presumably until some other body can develop rules that adequately address the many concerns around the use of the technology.

This draft commentary is one attempt to begin to bridge the divide between the moratoriums on the use of facial recognition technology and a comprehensive law regulating facial recognition technology. Specifically, our drafting team was charged with developing legal principles that should govern whether, under what circumstances, and what manner of, notice and consent of an individual should be required in connection with the collection, creation, use, and disclosure by the private and public sectors of that individual's biometric facial recognition data.

The primary intended audience for this commentary is United States state and federal legislators and other policymakers that are considering whether and how to regulate facial recognition technology, in particular, how best to implement new or amend existing notice and consent requirements in connection with the collection, creation, use, and disclosure of biometric facial recognition data. Public and private sector actors also may use this commentary as a source of considerations or best practices regarding the use and implementation of facial recognition technology.

At the outset, it should be understood that this commentary is not an attempt to craft overall privacy principles for the use of facial recognition technology. Our mandate was more narrowly

tailored. Instead, this commentary explores whether a notice and consent model—which is the prevalent model for U.S. privacy laws—is appropriate given the unique concerns posed by facial recognition technology and, assuming that it is in at least some instances, how lawmakers and policymakers should think about what constitutes appropriate notice and consent when using facial recognition technology. The concept of notice and consent is grounded in the notion that information privacy requires that individuals be able to choose whether and how others collect and use their information.¹ In order to allow such choice, individuals should be given sufficient information to understand what is being asked of them (*i.e.*, notice), and the ability to determine for themselves whether to accept the terms as presented (*i.e.*, consent).² This commentary sets forth guiding principles for what constitutes adequate notice and consent as they relate to the use of facial recognition technology, and explores the unique privacy considerations attendant to the use of facial recognition technology that may make reliance on a notice and consent model problematic in certain circumstances.

As is almost always the case with these commentaries, the drafting team did not address all aspects of the use of facial recognition technology. The drafting team only addresses facial recognition technology designed to compare facial images in order to determine whether they correspond to the same person (for identification or verification purposes). This commentary will not address facial analysis (where different facial images known to belong to the same individual are analyzed for a particular purpose, such as eye tracking),³ or facial detection (determining whether any human face is present in an image at all) standing alone. The drafting team also does not address biometric technologies other than facial recognition technology. Although many of these principles may be relevant for policymakers and lawmakers focused on other biometric technologies, the differences between those technologies and facial recognition technology may require additional protections for the use of facial recognition technology. Finally, this commentary also does not

¹ See Robert H. Sloan and Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, J. HIGH TECH. L., 148, at 373-74 (2013).

https://scholarship.kentlaw.iit.edu/fac_schol/568?utm_source=scholarship.kentlaw.iit.edu%2Ffac_schol%2F568&utm_medium=PDF&utm_campaign=PDFCoverPages.

² The notice and consent model is described as having its origin in the “fair information practice principles” (FIPPS) that were developed in the 1970s and early 1980s through the work of several advisory bodies. Fred Cate, *The Failure of Fair Information Practice Principles*, in *THE FAILURE OF FAIR INFORMATION PRACTICE PRINCIPLES* 342, 345-55 (Jane Winn ed., 2006). Although there are different iterations of the FIPPS, they all rely to some extent on the concept of notice and choice. For example, the Federal Trade Commission’s privacy principles developed to address the practices of online services include notice/awareness and choice/consent as two of the five core principles of privacy protection. Federal Trade Commission, *Privacy Online: A report to Congress* (1998).

³ Facial analysis systems are designed solely to work with sets of images that the system is to assume correspond to the same person (e.g., a system that is asked to compare an image or video of a given person against a baseline image or video of the same person with respect to behavior/motion, e.g. eye tracking, or changes in the person’s appearance); or a system designed to create theoretical images or data for a given person corresponding to a baseline image of the same person (such as with age-progression analysis/projection).

address considerations around notice and consent as they apply to minors or individuals with diminished capacity, as greater protections for those individuals may be recommended.

II. HOW FACIAL RECOGNITION TECHNOLOGY WORKS

Facial recognition technology is a type of biometric technology. Biometric technologies can be used to identify individuals based on one or more unique physical or behavioral characteristics. These characteristics can be static, such as a fingerprint or face; or dynamic, such as how a person types, speaks, or walks.⁴ In the broadest sense, facial recognition technology describes a computer system that can recognize, or match, images of faces. When such a computer system is combined with a camera input, facial recognition technology can also refer to a specific type of machine vision technology. In either case, the computing component of the system relies on a specific type of artificial intelligence called machine learning to perform the facial matching task.

In general, machine learning systems perform tasks based on a model built (at least in part) by the system itself. The computer system uses training data to learn how to better perform its expected task, without requiring explicit programmed instructions for every decision that it makes. The system may “learn,” *i.e.*, improve its algorithm, by evaluating its performance of a certain task, and then checking its work against the “answer key,” which may be a known data set in common use. Alternatively, system designers or users can give the system feedback on its performance, and the system may use this feedback to change its algorithm to improve its performance.

As used in this commentary, facial recognition refers to the following broadly defined use case and system:⁵

Step 1 (Capture or Enrollment). The user presents the facial recognition system with an image (whether a stored photograph/video still, or an image buffered from real-time video). In this commentary, the drafting team refers to the image the user presents to the system at the point of use

⁴ Other types of biometric identifiers may include DNA, retinal or iris (eye) patterns, fingerprints, hand or finger geometry, and voice, among others. Additionally, there are behavioral biometric identifiers, including Morse keystroke or typing cadence, gait, or signature recognition. Although this commentary focuses on facial recognition, legislatures and policymakers dealing with other biometric technologies may also find this commentary useful.

⁵ There are many differences in how facial recognition systems work, depending on how different trade-offs such as efficiency/speed, accuracy, cost, and other factors are balanced. So while this description may not be applicable in every respect to every facial recognition system in use or that may be developed, it is intended to be sufficiently abstracted so that it describes the vast majority of facial recognition systems currently in use.

as the “query” image, although this input image is also frequently referred to in the literature as the “probe” image.⁶

Step 2 (Facial Template Creation). Facial recognition technology does not involve a computer looking at a person or face in the same way that humans “look at” a person or a face. Instead, the system typically processes the images (both query and gallery) to create face templates, which are mathematical representations of the original image. The first step in this process is facial detection—in which the system determines whether or not a face is present in the image and, if so, where that image is located such that the facial features may be cropped and normalized to prepare for derivation of the facial template data.⁷ After a face is detected, the image is “normalized” to the maximum possible extent, by adjusting for lighting, camera angle, or even age discrepancies if possible, and eliminating “noise,” that is, fine details that are likely to vary between images of the same person and that make it difficult for the facial recognition system to identify significant patterns. After the system normalizes the image, it converts the physical features into a set of numerical data (a “facial template”) which maps the person’s unique facial features relative to each other, for example, in terms of distances, angles, vectors, and topographies. Facial recognition systems can use these numerical data sets to compare against the facial templates of other people.

Step 3 (Facial Template Matching). For any of a number of reasons, the user will wish to know whether the particular person captured in the query image is the same person depicted in an existing image⁸ already stored in or accessible by the facial recognition system. The existing image(s) against which to compare the query images reside in the facial recognition system’s “image gallery” or “gallery database.” The gallery database will typically contain a large number of images of people, *i.e.*, pictures of faces (or the numerical data derived from these pictures). Typically, each image in the image gallery will be associated with a particular known person; and some people may have more than one corresponding image in the image gallery.

⁶ See U.S. Government Accountability Office Report, *Facial Recognition Technology: Current and Planned Uses by Federal Agencies*, GAO-21-526, at 3 (August 2021).

⁷ While facial detection is used as a separate, stand-alone technology in many applications (where the technology user is only interested in determining whether any person’s face is present in an image or video feed and not identifying or verifying that person), it is also a necessary subcomponent of any facial recognition system. A facial recognition system cannot begin the process of recognizing a person’s face until it has determined where, if anywhere, a human face exists in the query image. As discussed previously, for purposes of this commentary, the drafting team has focused on facial recognition technology when it is used to make a determination as to whether two images correspond to the same person.

⁸ In some facial recognition systems, the system may merely store template data derived from images showing people, as opposed to the full images themselves, but for current purposes we will assume that all systems store full photographic images as opposed to simply derivative numerical template data.

Users can compare the query image against one, or many, images from the gallery database, depending on the user's goal:⁹

- When using the system to effect one-to-one matching, or “verification,” the user asks the facial recognition system whether the query image matches a particular single image from the gallery database. The most common example of such 1:1 verification will be when an individual presents their face to unlock a mobile phone or other computing device. As another example of 1:1 verification involving a large gallery, the user may be a traveler or immigration official presenting the query image of the traveler just taken at a national port of entry kiosk, to be compared against the single gallery image (also called a “reference image” in the verification context) of the traveler's official ID photo stored by the immigration agency.
- If, in contrast, when a user employs a facial recognition system for one-to-many matching, or “identification,” the user asks the facial recognition system whether the query image matches any of the large number of images of known people from the gallery database. For example, the user may be a law enforcement officer with a video still of an unidentified person of interest at a crime scene, to be compared against a gallery database of known people in order to generate potential leads for further investigation.

In either the “verification” or “identification” use case, “facial recognition” is the computing task, performed by the facial recognition system, of determining whether the person shown in the query image is likely to be the same person shown in the images from the gallery database. If the facial recognition system finds that this likelihood is high, this may be referred to as a “match,” a “hit,” or a “positive,” either by the system itself, or by the user. Depending on the system's/algorithm's characteristics, or selections made by the user or the user's organization/the system's owner, there is likely to be a minimum confidence/probability of match required before the system will confirm a match between the query image and the one or more gallery image(s) (a “positive”). These “positives,” when the facial recognition system has determined that the person in the query image is to some degree of likelihood the same person in one or more of the gallery images, are returned to the user as output; typically, with the full corresponding image from the image gallery for human reference.

⁹ Various algorithms have been implemented to perform this comparison, from more conventional, deliberately designed algorithms which are tested against sample data sets and refined in order to improve results. Alternatively, facial recognition systems may be implemented using a subset of machine learning systems called neural networks, such as convolutional neural networks (CNNs). Such systems are able to generate very similar template data for different images of the same person using data points developed by the neural network itself—it may not be entirely clear to the developers of the system exactly how these datapoints are used to create a template, or even what data points are being primarily considered. Empirically, however, these systems may prove to be more accurate than traditionally designed algorithms.

In the case of verification, (one-to-one matching), if the system is unable to match the query image to the gallery (or “reference”) image, this means that the query image was not validated (a “negative” result). Because of limitations in the algorithms used, or the quality of the available query image or gallery images, from time to time the system may not correctly match a query image to a gallery image, even though the images in fact correspond to the same person. If an image of the person in the query image is in the gallery database, but the system says that it cannot find it, that erroneous non-hit is a “false negative.” Alternatively, if the system returns a match (*i.e.*, reports that two images are quite likely to correspond to the same person¹⁰), but it turns out that the person in the query image was not in fact the same person returned by the system from the gallery database, this erroneous hit is called a “false positive.”

In the case of identification (one-to-many matching), if the system finds one or more potentially “matching” images from the image gallery, typically these images will be returned to the user as output, together with any information corresponding to the gallery images such as the names and other identifying information of the people depicted in the returned gallery images. Depending on the design and use of the system, the output to the user will usually also include the system’s confidence about the match (e.g., how “good” the match was in mathematical terms), and the query image, particularly if the person in the query image is not present at the use site. As with the verification application, a facial recognition system can make errors in its determination. In particular, the error rate (both of false positives and false negatives) disproportionately affects people of color and women.¹¹

III. USES OF FACIAL RECOGNITION TECHNOLOGY

The use of facial recognition technology for a wide variety of purposes has grown rapidly in recent years. This can be attributed to multiple factors, including rapidly evolving technology enabling the development of increasingly sophisticated software and other tools to conduct facial recognition, as well as global expansion of the availability and daily use of digital cameras for public and private purposes. In addition, decreased cost and improved performance and accuracy of facial

¹⁰ In practice, facial recognition systems do not typically make absolute statements of whether a match does or does not exist among the images in the system’s image database. Instead, like many biometric systems, facial recognition systems generally provide an assessment of the similarity of the faces in the images as a percentage, or a likelihood that a match has or has not occurred based on the data and model comprising the system. National Research Council, *BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES*, at 22, 31 (Joseph N. Pato and Lynette I. Millett eds., 2010). In addition to the system’s own probabilistic assessment included with any given match report provided to the user, the relative accuracy of a particular facial recognition system can also be described empirically with regard to the system’s “false match rate” (number of false positives as a proportion of total tasks) or “false non-match rate” over time. *Id.* at 26.

¹¹ See, *infra* Section V.A.

recognition systems has resulted in a proliferation of both the number and types of entities that may make use of facial recognition in myriad contexts.

Below are some current common uses of facial recognition technology, as well as emerging and potential uses, that may be taken into consideration when determining how to approach notice and consent requirements. The drafting team does not intend this list to be comprehensive; rather we highlight a broad range of scenarios in which facial recognition technology could be used and thus circumstances that a notice and consent framework would need to take into account.

- ***Law enforcement.*** Federal and state authorities may use facial recognition technology to identify potential suspects, as well as to identify missing persons or crime victims. In addition, law enforcement may use facial recognition technology to research information about individuals believed to pose a threat to national security.
- ***Private security.*** In the private sector, non-governmental entities may use facial recognition technology to identify individuals who pose a known or potential security risk. For example, a retailer may deploy facial recognition technology to flag an individual who previously committed a theft at the time that person enters the store, or a private security company may use facial recognition to identify a stalker within a crowd at a concert or sporting event.
- ***Private investigations.*** Operating outside the law enforcement setting, private investigators may deploy facial recognition technology to locate target individuals in various settings or to determine the identity of associates of targets who are otherwise unknown to the investigator.
- ***Access control and authentication.*** Facial recognition technology may be used to control access to electronic devices and physical spaces. A familiar example is the use of facial recognition technology to unlock a smartphone or to log in to a camera-enabled computer. Facial recognition technology may also be used to verify the identity of travelers at airports, and to authenticate the identity of employees entering a secure location in an office or factory.
- ***“Touchless” transactions.*** Once viewed more as a convenience than anything else, touchless interactions may have public health benefits. Facial recognition technology offers the ability to identify oneself and conduct transactions using a facial scan that does not require an individual to touch common surfaces or directly interact at close range with other individuals.

- ***Marketing and customer engagement.*** Retailers may use facial recognition technology to identify prominent individuals and/or loyal customers entering a store for purposes of ensuring that sales staff provide those individuals with exemplary service.
- ***Personal use by individuals.*** Access to facial recognition technology is likely to expand significantly with a variety of potential use cases for private individuals in their personal lives. For example, individuals can use facial recognition technology to search photo databases for doppelgangers or long-lost relatives, to track children/spouses/elderly family members in various settings, or to discover the identity of unknown individuals seen in public settings. In addition to ostensibly benign uses, facial recognition technology also could be used for stalking or harassment.

IV. CURRENT U.S. APPROACH TO REGULATING FACIAL RECOGNITION TECHNOLOGY

There is no comprehensive federal privacy law that specifically addresses the use of facial recognition technology. Instead, for federal applications, the Privacy Act generally regulates its use.¹² There are also state and local privacy laws that regulate the use of facial recognition technology by public and private sector entities. The drafting team identified the following types of laws that could apply to public sector or private sector uses of facial recognition technology depending on the particular circumstances:¹³

- **Privacy Act**
- **State data breach notice laws**
- **State biometric privacy laws**
- **State and local facial recognition restrictions or regulations**

For purposes of this commentary, the drafting team focused primarily on state and municipal approaches to regulating the technology as those were the most directly on point. Some states have enacted data breach notification laws that cover biometric information and require notice to individuals and (potentially) regulators in the event of a data breach. A small subset of states have

¹² Privacy Act of 1974, Public Law No. 93-579, as amended, codified at 5 U.S.C. § 552a. The Privacy Act generally prohibits, subject to a number of exceptions, the disclosure by federal public sector entities of records about an individual without the individual's written consent and provides individuals with a means to seek access to and amend their records.

¹³ An overview of some of the laws and ordinances identified and surveyed by the drafting team can be found at Appendix A.

enacted general privacy laws that cover facial recognition technology as biometric information, or passed general biometric privacy laws. Only Maine has banned the use of facial recognition technology statewide, though several other states and municipalities have cabined its use or imposed a moratorium for specific uses by police or other governmental entities. These different types of regulatory approaches are discussed in turn.

The most common approach from a state law perspective is not really aimed at facial recognition technology at all, but attempts to fold facial recognition technology into the broader set of biometric information already regulated by the state. The California Consumer Privacy Act (“CCPA”)¹⁴ may be the most well-known version of this type of statute, which defines protected personal information in such a way as to include unique biometric data. The CCPA is a broad privacy statute that, among other things, includes transparency requirements for businesses collecting personal information and provides certain privacy rights to individuals whose personal information is collected by businesses. The CCPA also imposes notification requirements on persons conducting business who maintain unencrypted and unredacted personal information and who become aware of security breaches, and imposes civil penalties in the case of a breach but not a private right of action. The inclusion of unique biometric data in the scope of the protected information would include facial recognition technology, but would also include other forms of biometric information. Arizona, Arkansas, Louisiana, New York, Oregon, and Washington have data breach notice laws with similar approaches.¹⁵

The other most common approach for the regulation of biometric information by state statute are biometric privacy acts, which include facial recognition technology as a regulated type of biometric data. For example, the Illinois Biometric Privacy Act (“BIPA”), enacted in 2008 to protect the privacy of personal biometric data, requires a company to post publicly a general notice about the company’s biometric data retention periods.¹⁶ BIPA also requires a company to provide specific notice and obtain consent from the particular person whose biometric information is collected,¹⁷ and bans the sale or trade of personal biometric information for profit.¹⁸ BIPA provides for a private right of action for anyone “aggrieved by a violation” of the statute.¹⁹ The Texas Business and Commerce Code § 503.001 similarly bans the use of biometric identifiers by companies without prior notice and consent, but provides for enforcement through a civil penalty of up to \$25,000 per violation to be brought by the Attorney General rather than through a private right of action.

¹⁴ The California Privacy Rights Act of 2020, which becomes effective in 2023, will revise and expand on the CCPA.

¹⁵ The Louisiana and Washington laws include a private right of action for a failure to timely notify in the event of a data breach.

¹⁶ 740 Ill. Comp. Stat. 14/15(a).

¹⁷ *Id.* at 14/15(b).

¹⁸ *Id.* at 14/15(c).

¹⁹ *Id.* at 14/20.

Some states have also imposed moratoriums on the use of facial recognition technology in particular areas or across the board. Maine is the only state thus far to comprehensively ban facial recognition technology. The Maine “[Act to Increase Privacy and Security by Regulating the Use of Facial Surveillance Systems by Departments, Public Employees and Public Officials](#),” holds that state, county, and municipal governments, including schools, are not allowed to use or possess any sort of facial recognition technology. It further restricts such entities from entering into a third-party agreement to obtain, access, or use facial recognition technology. It allows law enforcement to use the technology for investigating certain serious crimes, but bars state law enforcement agencies from implementing their own facial recognition technology systems. They may request facial recognition technology searches from the FBI and the state Bureau of Motor vehicles in certain cases.

Additionally, the law stipulates any unlawfully obtained data must be deleted, that it is inadmissible as evidence, and that the results of a facial recognition search are not sufficient, without other evidence, to justify “arrest, search or seizure.” The act also gives “injured or aggrieved” individuals the opportunity to seek “injunctive or declaratory relief” against a “department, public employee or public official” believed to be in violation of the law. A public employee or official who violates the law “may be subject to disciplinary action, including, but not limited to, retraining, suspension or termination.”

Other states have more limited bans or moratoriums. Vermont bans police use of facial recognition technology altogether, with a carve out for use in criminal investigations involving the sexual exploitation of children. Virginia prohibits local law enforcement and campus police from purchasing or deploying facial recognition technology unless expressly authorized by state statute. Massachusetts banned police use of facial recognition technology in criminal investigations, and [California Assembly Bill 1215](#) imposes a three-year moratorium on the use of facial recognition technology in police body cameras, and authorizes a private right of action against a law enforcement agency or officer who violates that prohibition.²⁰ New Hampshire and Oregon ban police from using facial recognition technology in body cameras used by police.

In addition to statewide actions, cities and municipalities across the country have enacted bans or moratoriums on the use of facial recognition technology, mostly by governmental entities and police. In California, the cities of Alameda, Berkeley, Oakland, and San Francisco have all banned the use of facial recognition technology by city agencies, including police. The bans vary somewhat in terms of scope and rules for use of facial recognition technology over time. Several Massachusetts cities—Boston, Brookline, Cambridge, Northampton, and Somerville—have similarly prohibited use of facial recognition technology by city agencies and employees. The [Boston Ordinance](#) includes a private right of action. King County, Washington (which includes 2.3 million people in and around Seattle) and Madison, Wisconsin, have also banned facial recognition

²⁰ The California moratorium went into effect January 2020.

technology used by government entities, though the Madison ordinance has a number of exemptions and carve-outs. The [City of Pittsburgh](#) enacted an ordinance that requires city entities, including police, to get city council approval of the use of facial recognition technology before they are acquired or used, except in “an emergency situation.” [New Orleans](#), Louisiana specifically banned the use of four pieces of technology in December 2020: facial recognition, characteristic recognition and tracking software, predictive policing, and cell-site simulators. And [Minneapolis](#) banned use of facial recognition technology by the Minneapolis Police Department in February 2021, while Jackson, Mississippi, preemptively banned the Jackson Police Department from using facial recognition technology to identify people in August 2020.

Finally, two cities named Portland have facial recognition bans worth discussing. The [City of Portland, Maine](#), enacted a preliminary ban on use of facial recognition technology by city employees in August 2020. Then, in November 2020, voters enacted a stronger ban on use of facial recognition technology by government employees by ballot initiative, which includes a private right of action and entitlement to \$1,000 in fines and seems to go farther than the Maine state statute. The [City of Portland, Oregon](#), enacted a ban on facial recognition technology use in September 2020 that not only prohibits government use but also restricts many applications of facial recognition by private companies. Effective January 1, 2021, Portland, Oregon banned private entities from using facial recognition technology in places of “public accommodation.”²¹ The Portland, Oregon ban contains a private right of action, with statutory damages of \$1,000 per day.²² A primary motivation for Portland in passing this ban, as articulated in the ordinance itself, was concern that “Face Recognition Technologies have been shown to falsely identify women and People of Color on a routine basis.”²³

The drafting team also considered proposed federal legislation that has come before Congress in recent years. Given the extent of concern over the use of facial recognition technology by government and private actors, there are surprisingly few federal legislative proposals introduced that address the use of facial recognition technology, and none of them take a comprehensive approach to its regulation. The approach taken by Congress to date in draft bills appears to be to either ban the use of the technology until a comprehensive law can be developed, prohibit its use in certain discrete circumstances (*e.g.*, police body cameras or in schools), or address particular concerns like the scraping of images from websites and their subsequent inclusion in commercial databases that can be used by the government and private entities. A description of three of the proposed federal bills can be found in Appendix B.

²¹ Portland, OR., City Code Ch. 34.10 (2020).

²² *Id.*

²³ *Id.*

V. RISKS OF FACIAL RECOGNITION TECHNOLOGY

The recent development of sophisticated facial recognition software has generated unique opportunities for public and private sector application of the technology, while also raising serious concerns about its threat to individual privacy and civil liberties that, in turn, poses challenges to businesses seeking to use the technology. We have organized our discussion of these risks below by first addressing potential risks to individuals and then describing the challenges businesses may face as they seek to make use of facial recognition technology.

A. Risks to Individuals

- **Over-Arching Privacy Concerns.** The use of facial recognition technology may raise privacy concerns depending on the facts and circumstances around its use. For example, the Federal Trade Commission has noted that deployment of the technology could end the ability of individuals to remain anonymous if deployed widely.²⁴ The concern is that if anyone can be identified in a crowd through the use of the technology, there is no opportunity for an individual to choose to remain anonymous without taking drastic measures, such as significantly changing their appearance or avoiding the particular public fora under surveillance, which becomes more difficult the more places that are under surveillance.²⁵ Other privacy related concerns that have been raised include the potential for the technology to be used in public places and in ways that are not obvious to those being surveilled—for example, sunglasses with facial recognition capabilities, or the potential for databases of photos or face templates to be breached.
- **General Constitutional Concerns.** When used for the purpose of law enforcement, facial recognition technology offers both promise and peril. When used with due regard for the principles that undergird the U.S. Constitution, the technology promises to assist in efficiently identifying targets of investigation, potentially improving the reliability of witness identification, and deterring crime. When used without due regard for Constitutional principles, however, the technology risks violating civil liberties and may confound

²⁴ See FTC Staff Report, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, at 7-8 (2012) (citing concerns of commenters).

²⁵ Evan Selinger and Woodrow Hartzog have recommended reframing this loss of anonymity as a loss of obscurity to better describe the transaction costs, or the ease or difficulty of finding information and correctly interpreting it. They describe obscurity as what allows us to foster individual autonomy by “selectively disclos[ing] information and sharing different aspects of our identity in different contexts” or allowing us to participate in certain activities without worrying about social stigma or recriminations by the government. Evan Selinger & Woodrow Hartzog, *The Inconsistency of Facial Surveillance*, 66 LOYOLA LAW REVIEW, at 101, 114-15 (2020).

successful prosecution by inviting legal challenges based on the Constitutional principles violated. Improper use of the technology might also escape judicial review and/or constraint and, thereby, tread on constitutionally protected rights without redress unless and until a legislature intervenes. Whether it is a court or a legislature that reacts to transgressive use of the technology, the result may be a range of ambiguous standards and/or unambiguous prohibitions that make it difficult or impossible to deploy the technology with confidence. Absent an established set of governing standards for the use of facial recognition by law enforcement, any decision to deploy the technology should be based on careful consideration of the ways in which a given use of the technology could transgress any one of the Constitutional principles discussed below.

- **Fourth Amendment Concerns.** The primary constitutional question surrounding any warrantless use of facial recognition technology by law enforcement to identify and surveil the activities of one or more individuals in space visible to the public is whether the use of this technology ever violates a person’s “reasonable expectation of privacy” under the Fourth Amendment.²⁶ As of September 2021, the U.S. Supreme Court has not directly addressed this question, but existing Supreme Court jurisprudence points to factors that the court might consider. Two relatively recent cases suggest increasing Supreme Court concern with the pervasiveness of the surveillance permitted by new technology: *U.S. v. Jones*, which involved the use of a Global Positioning System (GPS) tracking device;²⁷ and *Carpenter v. U.S.*, in which law enforcement used cell phone subscriber location information to place a defendant at the scene of several robberies.²⁸ Although many deployments of facial recognition will fail to implicate Constitutional concerns, the use of facial recognition

²⁶ *Katz v. U.S.*, 389 U.S. 347, 361 (1967).

²⁷ *U.S. v. Jones*, 565 U.S. 400 (2012). In *Jones*, the government, acting without a warrant, installed a Global Positioning System (GPS) tracking device in the vehicle of a suspected drug trafficker. The device tracked the movements of that vehicle 24 hours per day for 28 consecutive days. The Court found that the trespass into the vehicle required to install the GPS tracker rendered the tracking itself a search within the meaning of the Fourth Amendment, but two concurring opinions observed that “physical intrusion is now unnecessary to many forms of surveillance.” The concurring Justices asserted that the surveillance was sufficiently persistent, lasting four weeks, and pervasive, tracking every movement of the vehicle, that it should be deemed a search within the meaning of the Fourth Amendment even absent a trespass.

²⁸ *Carpenter v. U.S.*, 138 S. Ct. 2206 (2018). In *Carpenter*, 127 days of subscriber location information (that was continuously collected by a cellular phone service provider in their ordinary course of business) placed the defendant at each of several armed robberies. In holding that a warrant is required to collect cell-site location information over such a long period of time, Chief Justice Roberts, referring to the concurrences in *Jones*, noted that, “[a] majority of the Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements.” *Id.*, at 2209-2210. As of yet, no discernable norms have arisen in this jurisprudence, making it difficult to predict what *Carpenter* means for the use of facial recognition when used to track the location and activities of those subject to surveillance.

to evaluate imagery collected from multiple locations or persistently over time may suffice to violate an individual's Fourth Amendment rights.

○ **First Amendment Concerns.** Potential occasions for deployment of facial recognition are political protests or other events, which may implicate the right to assemble and/or right of free speech. Although camera phones and other forms of video surveillance are already widespread, a rise in the systematic recording and identification of individuals associated with these events may have a chilling effect on participation.²⁹ As of this writing, no court has yet recognized a constitutional basis to curtail this type of surveillance. Accordingly, legislatively established rules governing this use of facial recognition technology to meet legitimate law enforcement needs could be useful to ensure that the exercise of constitutionally protected rights is not suppressed.

○ **Due Process Concerns.** When law enforcement uses facial recognition to identify the perpetrator of a crime, the competency of that identification is likely to raise constitutional challenges related to the right to due process. That is, if the gallery database is skewed, if the algorithm is badly biased, or if the match parameters are insufficiently tight, the government should expect an argument that process is “so impermissibly suggestive as to give rise to a very substantial likelihood of irreparable misidentification.”³⁰ To date, the Supreme Court has not explored the relationship between facial recognition as used to identify a defendant and the existing jurisprudence regarding lineups and photo arrays. Generally speaking, when evaluating an identification procedure to determine if it was constitutionally sound, a court must consider: (1) whether the photo array procedure was unnecessarily suggestive; and (2) if so, whether the corrupting influence of the procedure was so suggestive that it outweighs the reliability of the identification. When a computer stands in place of a witness, the quality of the query image stands in place of witness perception. If facial recognition software overestimates confidence in matching or law enforcement officers define a match too loosely in terms of the system's statistical assessment of its match determination, a danger arises that jurors will wrongly perceive scientific certainty where no such certainty is warranted. Even software that is working exactly as it is designed may still misidentify the perpetrator

²⁹ There is mounting evidence that, in the absence of regulation, some law enforcement agencies continue to use the technology to develop dossiers on individuals not suspected of having committed any crime, ignoring or dismissing the chilling effect that this type of surveillance is likely to have on constitutionally protected activity. See Joanne C. Cavanaugh and Marc Freeman, [South Florida police quietly ran facial recognition scans to identify peaceful protestors. Is that legal?](#), (Jun. 26, 2021).

³⁰ See *Simmons v. United States*, 390 U.S. 377, 384 (1968).

of a crime. In this way, an algorithm trained on a biased data, or administered in a careless manner, may create an ongoing risk of a miscarriage of justice.

○ **Racial Bias.** There is growing evidence that some facial recognition systems suffer from racial bias. Facial recognition systems historically have had a difficult time detecting facial points on persons with darker skin complexions.³¹ A 2019 federal study of facial recognition databases used by law enforcement in the United States showed that “Asian and African American people were 100 times more likely to be misidentified than white men, depending on the particular algorithm and type of search.”³² Deficiencies in the technology have led to real world examples where facial recognition systems have misidentified people of color, leading to their wrongful detention or arrest.³³ Among other issues, many commonly used datasets contain imbalanced demographic distributions that result in biased discrimination when used to train facial recognition models. A database of images used to train the software may be so small and so racially skewed that the resulting algorithm is less reliable when matching people of color than it is in matching those of Anglo-European descent.³⁴ To the extent a gallery database queried is racially skewed, people of color are more likely to be matched to a query image because they represent a higher proportion of the images in the database than in the relevant population. This problem is exacerbated when matches are simply ranked, as this may lead law enforcement to direct investigative resources at the best of the matches even if the match is not particularly good, even by the system’s own admission.³⁵ These defects in facial recognition systems may operate to direct disproportionate investigative attention to people of color in a way that is functionally equivalent to racial profiling.

B. Challenges to Businesses

Separate from the privacy risks to individuals described above, businesses may face a variety of regulatory, legal, operational, reputational, and security challenges associated with their use of

³¹ See Larry Hardesty, [Study Finds Gender and Skin-Type Bias in Commercial Artificial Intelligence Systems](#), MIT News Office, (Feb. 11, 2018).

³² Drew Harwell, [Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use](#), WASH POST (Dec. 19, 2019).

³³ See <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>, Victoria Burton-Harris & Philip Mayor, American Civil Liberties Union, [Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart](#) (June 24, 2020); Bobby Allyn, NPR News, [The Computer Got it Wrong: How Facial Recognition Led to False Arrest of Black Man](#) (June 24, 2020).

³⁴ Harwell, *supra* note 34.

³⁵ Benjamin Conarck, [How an accused drug dealer revealed JSO's facial recognition network](#), The Florida Times-Union, [How an accused drug dealer revealed JSO's facial recognition network - News - The Florida Times-Union - Jacksonville, FL](#).

facial recognition technology. When making the decision to deploy facial recognition technology, companies must carefully weigh the potential benefits to their organization against these risks, which we have outlined at a high level below.

- **Regulatory Enforcement Risk.** As discussed in Section IV above, a number of laws and ordinances regulating the use of facial recognition technology have been enacted at the local and state levels in the United States. The regulatory landscape remains in flux, however, and as use of facial recognition technology expands, there is likely to be additional legislation in this area. When developing and/or implementing facial recognition technology, companies must consider which laws apply to their proposed use case(s) and implement appropriate compliance programs.

Most of the laws on the books do not include a private right of action, and thus are enforced by the relevant government regulator. An understanding of enforcement priorities, past and current investigations, and enforcement actions should inform the company's approach to deploying facial recognition technology solutions. To provide a recent example, in January 2021, the Federal Trade Commission (FTC) entered into a settlement agreement with Everalbum after the FTC alleged that Everalbum's grouping and tagging of photos in its application without affirmative consent violated Section 5 of the FTC Act.³⁶ Everalbum enabled this feature on users' accounts by default, despite publicly stating that it "would not apply facial recognition technology to users' content unless users affirmatively chose to activate the feature."³⁷

Litigation Risk. In recent years, there has been a sharp rise in class action litigation related to the misuse of facial recognition technology, largely under Illinois's Biometric Information Privacy Act. One of the most notable lawsuits brought under Illinois's BIPA was a class-action lawsuit brought by Illinois consumers claiming that Facebook collected and stored the biometric data of millions of consumers without their consent as part of Facebook's "tag suggestions" feature.³⁸ Facebook eventually settled this case for a landmark \$650 million.³⁹ Although this case is an outlier in terms of size, this type of class-action suit is by no means rare.

- **Operational Challenges.** The implementation and use of facial recognition technology can be costly, time-consuming, and may require greater training and customization than

³⁶ *In the Matter of Everalbum, Inc.*, File No. 1923172 (FTC Jan. 11, 2021).

³⁷ *Id.*

³⁸ *In re Facebook*, 2018 U.S. Dist. LEXIS 81044, at *3.

³⁹ See Jennifer Bryant, *Facebook's \$650M BIPA settlement 'a make-or-break moment'*, IAPP (Mar. 5, 2021), <https://iapp.org/news/a/facebook-650m-bipa-settlement-a-make-or-break-moment/>.

expected.⁴⁰ Organizations must confront the time and cost of implementation, the accuracy of the technology, how best to protect the biometric data from a potential breach, and how to address effectively the regulatory and legal risks outlined above.⁴¹ Businesses may be surprised by the amount of time and money it takes to enroll large numbers of individuals into a facial recognition program. In addition, facial recognition technology functions best in highly controlled settings.⁴² In less controlled settings, such as when there is bad lighting or where faces may be obstructed, the likelihood of misidentification increases.⁴³ These technical limitations, along with concerns relating to discriminatory bias inherent to some datasets, are dangerous when combined with the potential ramifications to individuals of misidentification. For example, as explained above, there are examples of individuals, typically women and/or people of color, who have faced wrongful legal action on the basis of a misidentified facial scan.⁴⁴

- **Reputational Risk.** Whether or not a company faces regulatory scrutiny or a civil lawsuit, its use of facial recognition technology has the potential to backfire in the court of public opinion. As perceived risks to personal privacy and autonomy become more widely known and understood, an increasingly wary populace may view certain uses of facial recognition technology by private actors to be problematic or even invasive. Intentional or inadvertent misuse of this technology, not to mention errors in how the implementation functions that may result in real-life consequences for individuals, may draw undesirable attention to a company, including negative press coverage that could tarnish an otherwise well-respected brand or result in other reputational harm.
- **Security Risk.** Additionally, facial recognition also presents significant data breach risk in the event of cyberattacks. Given the sensitive nature of biometric data, an unauthorized disclosure can present significant risk of harm to consumers. In addition to the loss of facial recognition data, unauthorized access to biometric information can also trigger state data breach notification laws that have specific notice requirements and may include a private right of action that can lead to potentially significant damages when an entity fails to adequately protect biometric data.⁴⁵ Entities interested in using facial recognition technology

⁴⁰ See Arthur Piper, *About Face: The Risks and Challenges of Facial Recognition Technology*, Risk Management Magazine (Nov. 1, 2019), <https://www.rmmagazine.com/articles/article/2019/11/01/-About-Face-The-Risks-and-Challenges-of-Facial-Recognition-Technology->.

⁴¹ *Id.*

⁴² See William Crumpler, *How Accurate are Facial Recognition Systems – and Why Does It Matter?* Center for Strategic & International Studies (April 14, 2020), <https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter>.

⁴³ *Id.*

⁴⁴ See, e.g., K. Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, NY TIMES (Dec. 29, 2020).

⁴⁵ See 2021 Security Breach Legislation, National Conference of State Legislatures, <https://www.ncsl.org/research/telecommunications-and-information-technology/2021-security-breach-legislation.aspx>.

in their organizations must carefully assess their implementation strategy and ensure that the facial recognition tool will meet the organization's needs without exceeding the organization's risk appetite.

VI. Existing Principles and Best Practices

A number of organizations have developed best practices and general principles for using facial recognition technology. The drafting team surveyed these materials to understand existing guidance in this area and how these principles approach notice and consent. Each of the principles we reviewed relied on some manner of notice and consent, with some principles providing a more detailed description of what would constitute adequate notice and consent and others giving only cursory treatment to the reasoning and considerations behind the guidance. The majority of the principles that our drafting team identified and surveyed addressed the use of the technology in commercial applications. Below is an overview of some of the principles that we considered.

- The World Economic Forum's White Paper *A Framework for Responsible Limits on Facial Recognition Use Case: Flow Management* included a first version of principles that are an initial attempt to establish a governance framework for facial recognition technology.⁴⁶ The principles are bias and discrimination, proportional use of facial recognition systems, privacy by design, accountability, risk assessment and audit, performance, right for information, consent, notice and consent, right to accessibility and children's rights, and alternative option and human presence. The consent principle states that "[i]ndividuals should provide informed, explicit and affirmative consent for the use of facial recognition systems," and that "[e]nd users should have access to their personal biometric data upon request."⁴⁷ The notice and consent principle states that when facial recognition technology is used in public spaces, "clear signage should be deployed to ensure an obvious communication with end users on the use of facial recognition."⁴⁸ It also explains that areas where facial recognition systems are used should always be delimited and indicated to individuals, and that a "visual sign should also inform individuals when the system is in operation."⁴⁹

⁴⁶ World Economic Forum White Paper, *A Framework for Responsible Limits on Facial Recognition Use Case: Flow Management* (February 2020), available at http://www3.weforum.org/docs/WEF_Framework_for_action_Facial_recognition_2020.pdf. The first version of the principles are part of a larger multi-stakeholder effort to define the responsible use of facial recognition, and are intended to be reviewed and updated based on an 18-month pilot project.

⁴⁷ *Id.* at 8.

⁴⁸ *Id.*

⁴⁹ *Id.*

- The FTC issued recommended best practices for facial recognition technology in its *Best Practices for Common Uses of Facial Recognition Technologies* staff report.⁵⁰ The best practices in the report are intended to provide guidance to commercial entities either already using or planning to use facial recognition technology, and do not address uses by the public sector. The best practices put forth by the agency are that companies should (1) maintain reasonable data security protections for consumers' images and the biometric information collected from those images to enable facial recognition, (2) establish and maintain appropriate retention and disposal practices for the consumer images and biometric data they collect, and (3) consider the sensitivity of the information when developing their facial recognition products and services.⁵¹ The FTC also emphasized the need for simplified consumer choice and transparency. The report generally advocates that consumers be presented with clear notice about how the facial recognition features work, what data will be collected, and how that data will be used.⁵² The report also recommends providing consumers with a meaningful choice—in other words that some form of consent should be obtained prior to the use of facial recognition technology. This choice means that consumers should be able to opt out of the use of facial recognition technology, turn off the feature at any time, and have their data deleted upon opt out.⁵³ The FTC report also envisions affirmative express consent being necessary in two scenarios.⁵⁴ First, where the company is using consumer data in a materially different manner than claimed when the data was collected and, second, where the company would be using the technology to identify anonymous images of a consumer to someone who could not otherwise identify him or her. The justification for the latter is the significant privacy and safety risks that could accompany such uses.
- In 2016, the National Telecommunications and Information Administration (NTIA) released its *Privacy Best Practice Recommendations for Commercial Facial Recognition Use*, based on the Fair

⁵⁰ Federal Trade Commission, *Staff Report on Best Practices for Common Uses of Facial Recognition Technologies* (2012), available at <https://ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf>. The audience for the best practices were commercial entities, and not necessarily lawmakers and policymakers. The FTC also made clear that the best practices were not intended to be enforceable to the extent they went beyond existing legal requirements. *Id.* at 2.

⁵¹ *Id.* at ii.

⁵² *Id.*

⁵³ *Id.*

⁵⁴ Requiring affirmative express consent in these scenarios is consistent with the approach taken by the FTC in its 2012 Report Protecting Consumer Privacy in an Era of Rapid Change, available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>. That report explains that affirmative express consent could be obtained by presenting consumers with a “clear and prominent disclosure, followed by the ability to opt in to the practice being described.” *Id.* at 57, n. 274.

Information Practice Principles.⁵⁵ The principles apply only to commercial uses of the technology, and they explicitly carve out security applications (even if done for a commercial purpose), law enforcement, national security, intelligence, or military uses. Relevant to the concept of notice and choice, the transparency principle encourages covered entities to “make available to consumers, in a reasonable manner and location, policies or disclosures describing such entities’ practices regarding collection, storage, and use of facial template data.”⁵⁶ The principles explain that these should describe the reasonably foreseeable uses for the technology, the covered entities’ data retention and de-identification practices, and how an individual can review, correct, or delete their facial template data, where the covered entity offers such an option.⁵⁷ Although these principles do envision covered entities providing notice to consumers, they do not provide consumers with any meaningful choice. There is no ability to opt out or requirement that consumers consent in any meaningful way. When covered entities make material changes to their facial template data management practices, the principles encourage them to update their policies or disclosures, though affirmative express consent is not required.⁵⁸ The use limitation states that in cases where the technology is being used to determine an individual’s identity, covered entities are encouraged to provide the individual the opportunity to control the sharing of their facial template data with an unaffiliated third party that does not already have this information.

- The Future of Privacy Forum has also released *Privacy Principles for Facial Recognition Technology in Commercial Applications*.⁵⁹ There are seven principles that are outlined: (1) consent, (2) use - respect for context, (3) transparency, (4) data security, (5) privacy by design, (6) integrity and

⁵⁵ National Telecommunications and Information Administration (NTIA), Privacy Best Practice Recommendations for Commercial Facial Recognition Use, available at https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recognition.pdf. Although the best practices were intended to reflect a multi-stakeholder process, civil society organizations that initially participated withdrew their support for the process. In their statement on the best practices, many of these organizations criticized the best practices for failing to provide guidance for businesses and offering no real protection for consumers. Press Release: Joint Statement of Alvaro Bedoya, Center for Digital Democracy, Common Sense Kids Action, Consumer Action, Consumer Federation of America, Consumer Watchdog, Privacy Rights Clearinghouse, and U.S. PIRG, *Statement on NTIA Privacy Best Practice Recommendations for Commercial Facial Recognition Use* (June 15, 2016), available at https://consumerfed.org/press_release/statement-ntia-privacy-best-practice-recommendations-commercial-facial-recognition-use/. The statement explains that the stakeholders could not reach consensus on whether consent should be required, and takes issue with the fact that the best practices do not provide suggestions for how to evaluate and deal with the many issues that the use of facial recognition technology in commercial applications might raise.

⁵⁶ *Id.* at 2.

⁵⁷ *Id.* at 2.

⁵⁸ *Id.* at 2.

⁵⁹ Future of Privacy Forum, *Privacy Principles for Facial Recognition Technology in Commercial Applications* (September 2018), available at <https://fpf.org/wp-content/uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf>. The FPF principles are described as “intended to set industry best practices, inform consumer expectations, and educate policymakers.” *Id.* at 1.

access, and (7) accountability. The consent principle is to “obtain express, affirmative consent when: 1) enrolling an individual in a program that uses facial recognition technology for verification or identification purposes; and/or 2) identifying an individual to third parties who would not otherwise have known the individual’s identity.”⁶⁰ The principles explain that consent should be collected for verification (one-to-one matching) upon enrollment in the database, and that consent for identification (one-to-many matching) should occur prior to the matching process being initiated.⁶¹ The principles do envision certain circumstances where no consent is required, specifically collections of data for physical security, fraud, and asset protection programs or within a service provider relationship.⁶² The principles also envision circumstances where notice is required, but opt-out consent is sufficient. These included templates created within on-line platforms that may identify users to each other when the affected user accounts were already linked through an intentional connection or action by the individual users.⁶³ The principles also state that companies implementing facial recognition systems should provide consumers with meaningful notice about how the facial recognition software templates are created and how such data will be used, stored, shared, and maintained. The principles explain that, among other things, the notice should help consumers understand the purposes of the collection, whether the data may be shared, retention, deletion, or de-identification policies for facial recognition data, choices consumers may have, and which third-party partners receive the data.⁶⁴ The principles also envision that notice may differ based on the context, but that where appropriate, contextual and just-in-time notices should be used.⁶⁵

VII. PRINCIPLES

A. The use of facial recognition technology may pose unique privacy concerns, especially in the context of public sector use

The animating, underlying concern that drives much of the criticism of facial recognition technology is the potential for its use to infringe on an individuals’ privacy in a way that may not be present with other forms of biometric technology. As a result, the drafting team started from the

⁶⁰ *Id.* at 3. The FPF explains that “[e]xpress affirmative consent may be written or oral. Simple acceptance of a privacy policy or terms of service notice may not constitute consent if facial recognition is not clearly intrinsic in the service provided. Likewise, simply allowing one’s photo to be taken, without clear acknowledgement of the notice about the use of FR technology for that photo, is not sufficient.” *Id.* at n. 7.

⁶¹ *Id.* at 3.

⁶² *Id.* at 4.

⁶³ *Id.* at 4.

⁶⁴ *Id.* at 6.

⁶⁵ *Id.* at 6.

perspective of taking that concern seriously and considering what guidelines, if any, would stem from doing so.

1. *Public sector actors may not be similarly situated to private actors in many of their actions, positions, and coercive power.*

The drafting team considered both public and private sector uses of facial recognition technology. Many of the principles discussed in this commentary may have applications in both of those contexts, as well as other potential spaces. However, legislators and policymakers should recognize that public sector actors may not be similarly situated to private actors in many of their actions, positions, and coercive power. In addition, the ability to separate governmental and commercial use cleanly is not as simple as it may seem at first: public sector actors often engage in partnerships with private entities, purchase technology from commercial companies, or, on the flip side, engage in behaviors that more closely mimic a commercial enterprise. However, in many contexts, public sector entities may not be similarly situated to private actors in their actions, positions, and coercive power in the use of facial recognition technology. Law enforcement is the most obvious example of this difference, and it is, as a result, not surprising that most of the efforts to regulate government use of facial recognition technology at the state and local level regulate the police power, an area traditionally left to the states under principles of federalism. Law enforcement agencies have investigative powers, coercive power, and constitutional requirements that may not apply to commercial actors.

Government use of facial recognition technology for national security purposes, as well, may have different benefits (for example, spying, state secrets, needs in combat or warfare), different restraints (for example, constitutional restrictions, international treaties, rules of combat), and different public transparency concerns (for example, modified need for warrants or other oversight, civilian military relations and deference, use in relation to torture). On the other hand, as discussed more herein, when government acts like a business or private entity, the same restrictions and principles that apply to commercial actors may be appropriate for those government uses. In addition, following a robust notice and consent regime may be valuable for public sector actors as well. But when considering principles related to a notice and consent regime for the use of facial recognition technology, it is worth parsing out what forms of notice and consent are appropriate for government use, and what may need to be modified or reconsidered.

2. *The relevant question for many governmental uses of facial recognition technology may not be based on the adequacy of notice and consent.*

One overarching consideration is whether certain public sector uses of facial recognition technology, such as those in national security, law enforcement, or any action involving a fundamental constitutional right, lend themselves to a notice and consent regime. Rather, in those instances, the relevant question for legislators and policymakers may be whether the use of facial

recognition should be permissible at all, or subject to a different regulatory regime, and not whether notice and consent have been obtained. For police, for example, the question may be whether police officers may use facial recognition technology at all, or only in particular circumstances. Vermont's state regime related to law enforcement use of facial recognition technology is an illustrative example. Vermont banned the use of facial recognition technology by law enforcement except with prior authorization. The next year, law enforcement asked for and received authorization to use facial recognition technology in child exploitation cases, subject to some parameters, and the legislature considered claims from law enforcement that facial recognition technology was helpful for face matching and other mechanisms for enforcing child exploitation laws and use was tailored. In this instance, the relevant question is not whether notice and consent have been obtained, but rather, what the appropriate use of the technology is given law enforcement needs and constraints. Vermont police, presumably, do not want potential child exploiters being aware that they are being investigated—as a result, they are not interested in notifying suspects individually of the use or obtaining their consent. However, the state of Vermont has indicated that it does not otherwise believe that the use of facial recognition technology by law enforcement is permitted and that any specific use should be authorized by legislative action. Legislators considering the use of facial recognition technology by government entities, as a result, may be faced with different considerations, which may include but are not limited to: constitutional requirements, transparency, reliability of sources of information purchased from commercial entities, cost, potential for government overreach or misuse, democratic buy-in and legitimacy, and separation of powers. The drafting team has discussed these uses and identified some areas where these considerations may be present: law enforcement, national security, fundamental constitutional rights, and required public access and accommodations. This list, however, is not exhaustive.

For these applications, legislators and policymakers may find government use of facial recognition technology to be inappropriate in all circumstances, to be permissible by default, or to need separate governing standards. Given the privacy interests discussed above, the conclusion that government use of facial recognition technology should be permissible by default may not be compatible with the protection of privacy-based constitutional concerns in the United States. Some of the potential governing standards in situations where neither an outright ban nor unfettered use is preferred may be heightened accountability and transparency requirements, a warrant requirement, an establishment of court oversight, or the creation of separate courts similar to Foreign Intelligence Surveillance Act (“FISA”) courts. Government entities may also need to consider whether the privacy interest compels a conclusion in which entities presume that persons would not or did not consent to the use of facial recognition technology and then must justify the use based on the governmental purpose served. Notice and consent may be part of the considerations to be discussed or taken into account, but may be neither necessary nor sufficient to justify the use of the technology by a governmental entity.

3. *Notice and consent may not be an appropriate regime when the individual does not have control over the situation in some manner.*

One relevant question for legislators and policymakers considering parameters for governmental use of facial recognition technology (given the conclusion above that a notice and consent regime may not be appropriate for all government uses of facial recognition technology), is how to tell when an application or use of facial recognition technology by a government entity does warrant use of a notice and consent regime. Many government uses of facial recognition technology may involve people whose relationship with the federal government may not make true consent possible: criminal defendants, accused lawbreakers, people seeking government benefits, children, people seeking access to public locations or locations for which there is a constitutional right to access. In those instances, as noted, focusing on consent may not capture the risks and benefits of using facial recognition technology. Children, for example, are required to attend school. Providing notice and requesting that children consent to the use of facial recognition technology in order to access a public school building, for example, may not allow for true consent, given that children are required to be there and that children might not yet be of the age to be able to legally consent. Providing notice and requesting consent for use of facial recognition technology in order to make bail or as a condition of probation may not be a meaningful form of consent given the coercive position of the state vis a vis the criminal defendant. In contexts where people seek governmental benefits, consent may also be less meaningful. A person who is requested to allow use of facial recognition technology in order to access food for their otherwise hungry selves or children may not be in a position to meaningfully consent to that use. These examples are not identical, and some may implicate constitutional rights more than others. This commentary does not suggest that the use of facial recognition technology by a government entity ought to be banned outright or otherwise restricted. However, it does counsel that, given the lack of control the person subject to governmental action has over the situation or the nature of the relationship between the two, a notice and consent regime may not capture all of the issues at stake, and that a discussion of the benefits and drawbacks of use beyond notice and consent may be appropriate.

4. *A notice and consent regime may be appropriate for government uses of facial recognition technology in certain circumstances, such as where the government is acting in a manner analogous to a commercial entity, and the use does not implicate constitutional concerns or collective autonomy.*

Public sector applications of facial recognition technology typically will not lend themselves to a notice and consent model, and thus are likely better regulated by an accountability/transparency framework.⁶⁶ By contrast, to the extent that public sector uses are analogous to private or commercial uses, there is no inherent reason that a notice and consent regime cannot be implemented merely because a government body owns or operates the facial recognition technology system. Generally, notice and consent may be appropriate when the government's facial recognition technology is being used in connect with a service that is optional from the perspective of the public. In other words, notice and consent it may be appropriate when the public approaches the

⁶⁶ See *infra* Section VII.D.

government service as consumers with a true choice about whether or not they wish to use the service.⁶⁷ In general, such service offerings by government entities may be quite rare, particularly at the federal and state level. Where the government cannot implement a meaningful notice and consent system, then it will usually be appropriate instead for legislators and policymakers to consider an approach that monitors and regulates the government's use of facial recognition technology, as discussed elsewhere in this commentary. Typically, other parts of the government will carry out this accountability, answerable ultimately to the governed.

In order for an individual to have a legitimate choice about the use of a service, a number of criteria must likely be met. *First*, the government service should not be a monopoly, whether created by law or in fact, particularly when the service involves something reasonably characterized as a modern necessity. If a government body is planning to adopt a commercial notice and consent framework (for example, in lieu of being accountable to other governmental bodies under a transparency framework), the service offering provided by the government should not be a monopoly under a meaningful market definition, and in particular must not provide a service that is reserved to the government *de jure*. If the service is of a type that as a practical matter is a *de facto* governmental monopoly because of, for example, economies of scale, structural market conditions such as capital requirements, regulations, or subsidies (mass transit is an example), it may well be similarly impossible to apply a true consent regime under the circumstances.

Second, the government service should not be necessary to the exercise of fundamental rights. In order for a consent framework to be meaningful in a government application, the public's use of the service must not be necessary to the exercise of a fundamental right, either directly or indirectly. Therefore, for example, it would not be possible to obtain meaningful "consent" from a member of the public if we conditioned the right to vote on nominal "consent" to be subject to facial recognition technology at the polling place, even though the act of voting is wholly voluntary. Extending this concept to the indirect case, even if we ignore for the moment that each U.S. state has a monopoly on the issuance of driver's licenses and state IDs within that state, it also would not be reasonable to assert that a member of the public gave meaningful consent to submit to the use of facial recognition technology when applying for a state driver's license or state ID, if it is necessary to present such ID in order to exercise the right to vote.

Third, the government service and use of facial recognition technology should not, in practical effect, have a disparate impact on a historically disadvantaged group. Applicants for certain forms of public assistance, such as housing choice vouchers or benefits under the Supplemental

⁶⁷ The importance of whether a data subject's "consent" to enrollment is truly voluntary in the context of a government application of facial recognition technology is particularly critical when one considers that a government use notice and consent form is more likely than true consumer applications to notify the data subject that the enrollment data will be shared with law enforcement. For example, a Texas statute provides that a biometric identifier like a facial template that is captured for a commercial purpose cannot be shared with law enforcement except in response to a warrant (or as otherwise provided by state or federal statute). TEXAS BUSINESS & COMMERCE CODE, Title 11, Subtit. A., Ch. 503.

Nutrition Assistance Program⁶⁸ are likely to be of lower socio-economic status (SES); indeed, such concurrent status is generally a chief requirement for benefits eligibility under such programs. Viewing SES broadly across several criteria, racial and ethnic groups that face discrimination in the U.S. tend to be of lower SES than whites on average.⁶⁹ The prospect of a stratified society in which the less well-off simply cannot afford the same degree of personal privacy as those who are better off, and the less well-off are more frequently enrolled in facial recognition databases (which could potentially be made available to law enforcement) than the population as a whole is problematic. The fact that this effect could be correlated with racial or ethnic characteristics is of heightened concern. This is particularly so in light of empirical findings that many facial recognition systems have been designed and trained in a deficient manner, such that they perform poorly with non-white, non-male subjects, the characteristic of these systems which has led to a moratorium on their use in many states and municipalities, as discussed above.

In addition, when considering whether a public sector use is appropriate for a notice and consent model, legislators and policymakers should consider whether the public sector service would implicate and/or impinge on the exercise of individuals' First Amendment rights to speak/assemble. One can imagine this arising in a number of scenarios. For example, the U.S. National Park Service may not be thought by many to have a monopoly on places to enjoy outdoor recreation, and it is perfectly possible to avoid the U.S. National Park System. However, if the Park Service determined that as a public safety measure it wished to impose a notice and consent framework with mandatory facial recognition enrollment as a condition of entry into all U.S. National Parks, this could have vastly different implications for the National Mall, where protests take place, when compared to Yosemite and Yellowstone. Legislators and policymakers should therefore consider whether a facial recognition use that creates a risk of a chilling effect on the exercise of a First Amendment right such as freedom of speech or assembly is ever likely to support a valid notice and consent framework.

B. Actual notice should be meaningful and transparent

As discussed throughout this commentary, legislators and policymakers should recognize the importance of providing meaningful notice before using facial recognition technology on an individual, where such a notice and consent framework is appropriate. This is because facial recognition technology, while a powerful tool, can pose a substantial risk to an individual's privacy and civil liberties. As such, individuals should be given a meaningful opportunity to understand

⁶⁸ https://www.hud.gov/topics/housing_choice_voucher_program_section_8; <https://www.fns.usda.gov/snap/supplemental-nutrition-assistance-program>.

⁶⁹ Williams, et al., (2016), "Understanding Associations between Race, Socioeconomic Status, and Health: Patterns and Prospects" <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4817358/>.

what is being asked of them, and to choose whether or not to be subject to facial recognition technology.

For private and public sector entities providing actual notice of their use of facial recognition technology, those entities should provide the notice apart from other legal or financial disclosures, so that individuals recognize what the entities ask of them. In addition, they should present the notice in clear terms that are easily understandable. At a minimum, legislators and policymakers should consider requiring the following in any actual notice:

- That facial recognition data may be collected, captured, or otherwise obtained from an individual;
- The purposes for which facial recognition technology is being used;
- The purposes for which facial recognition data is collected;
- How facial recognition data is protected, including providing retention, deletion, or de-identification policies;
- Whether facial recognition data may be shared, transferred, sold, or otherwise disclosed to any third party;
- Whether requests can be made to delete or destroy a person's facial recognition data, and if so, how to make such a request; and
- Whether facial recognition may be shared with law enforcement.

With this information, individuals can make an informed decision to have (or not have) their biometric information collected, used, sold to or shared with third parties, and stored and maintained.

C. Individual consent for the use of facial recognition technology should be obtained wherever possible

Although the drafting team determined there were certain circumstances in which notice and/or consent for the use of facial recognition technology may be impractical or ineffective, or may not be the correct framework for evaluation, the default is that individual consent should be obtained prior to the use of facial recognition technology.⁷⁰ This general principle, however, is

⁷⁰ For the purposes of these Principles, the drafting team assumed that some level of “consentability” is achievable in the context of facial recognition, although recent commentators have questioned whether an individual can truly give knowing consent to the use of the technology. *See generally* Selinger & Hartzog, *supra* note 25.

subject to several underlying considerations that legislators and policymakers should address to ensure that such consent is valid and workable.

Legislators and policymakers should consider how the timing, form, and scope of consent may differ depending on a number of factors, including the risk to the individual under the circumstances. On one end of the spectrum, consent requirements could be met through mere notice in a privacy policy or terms of use, with the opportunity to opt out, effectively obtaining consent by mere use of services or participation in an event. On the other end of the spectrum, valid consent may need to be written, explicit, and affirmative, requiring a party to sign an instrument (physically or electronically) assenting to the use of facial recognition, perhaps at various stages in the facial recognition process and with finite periods of validity. Even if consent is more explicit, legislators and policymakers should consider whether the mechanism may assume consent by default (for example, a pre-check box on a web form) or whether a more affirmative method is required (for example, signing a hard copy form, clicking on an uncheck box, etc.). Ultimately, the risks posed to the individual by facial recognition technology should drive the timing, form, and scope of the consent required under the circumstances. In other words, depending on the technological activity and proposed uses of facial recognition technology, legislators and policymakers may find that consent could take on different characteristics.

1. *Adequate consent may vary by stage.*

One important risk factor that may drive the nature of any required consent is the stage in the facial recognition process: (1) facial image capture, (2) creation of a facial template, (3) association of a facial template to an identity, and (4) facial template matching (verification or identification). Each of these steps bears unique risks and may justify the use of more (or less) stringent consent mechanisms.

Consent to Image Capture. The individual and societal risk of image capture (effectively, collection of image or video data, without any biometric analysis) is low and—barring a wholesale rethinking of video surveillance in the United States—requiring explicit consent is least necessary. This understanding is based on a generally (although not universally) accepted belief—at least in the United States—that an individual should have no expectation of privacy in their image in a public setting. Requiring consent for mere capture would also generally upend the rights of entities to monitor their premises for security. There may, however, be circumstances where requiring consent for mere image capture would be more practical and reasonable. For example, a private entity could be required to obtain consent to capture an individual’s facial image when the individual is logging onto an online service from a private space, such as their home or office.

Consent to Create Facial Templates. The risks posed by the programmatic creation of facial templates may justify a requirement to obtain some form of individual consent. Unlike mere capture, once a facial template is created and stored, it is subject to uses beyond mere human-

verifiable identification. It is at this point all other uses of facial recognition technology become possible, opening the door to the numerous risks detailed above in Section V. Nevertheless, these risks may be relatively limited. Without associating a facial template to a specific identity, the risk of a data breach leading to identity theft is mitigated. Similarly, if the facial template is not used for identification and/or verification, the likelihood of bias leading to immediate, individual repercussions is reduced. Nevertheless, because the creation of a facial template opens the door to these subsequent uses as well as uses that have not yet been conceived of, there is a risk posed by long-term, inherent bias and subsequent misuse, including unconsented identification and verification. Although explicit, affirmative consent may be required at this stage, legislators and policymakers should consider a requirement that, at a minimum, individuals have the right to opt out of having their faces reduced to facial templates.

Consent to Associate Facial Template to an Identity. Overlapping with traditional notions of data privacy, legislators and policymakers could consider a requirement that explicit consent be obtained when a facial template is to be associated with an individual's identity using other personally identifiable information such as a name, address, phone number, Social Security Number, or even non-standard identifiers such as rewards program IDs or internet browsing caches. The risks posed by such association may be understood by the general public, but may still merit a more stringent consent mechanism. For example, although individuals may understand the general risk of identity theft under the circumstances, they may not appreciate how the unauthorized use of a facial template could make the impact of identity theft more severe. A requirement for affirmative, explicit consent strikes closer to the heart of concerns and criticisms of facial recognition technology, which often center on individual privacy. Inherent in this scope, however, is the murkiness of the definition of "identity." Should "identity" encompass, for example, temporary key numbers that allow a system to track or log a facial geometry? Most current privacy laws would, indeed, deem such a number "personal information." To require consent to assign such an identifier would arguably encompass every facial template. One way to square this circle may be to exempt "[l]imited collection/limited use programs that create or collect facial template data tied to a unique persistent identifier . . . if the identifier is not linked or linkable to any other personally identifiable information, including purchase or payment data."⁷¹ It could also be argued that a facial template itself constitutes uniquely identifiable information that is inherently subject to heightened consent requirements. Alternatively, at least for the purposes of facial recognition, "identity" could be more narrowly defined to encompass only information external to a facial geometry capturing system (e.g., name, Social Security Number, email address).

Consent to Facial Template Matching. The most stringent consent requirements may be reserved for the use of facial recognition to perform identification (one-to-many) and verification

⁷¹ Programs that "create or collect facial template data tied to a unique persistent identifier . . . if the identifier is not linked or linkable to any other personally identifiable information" may also fall into this risk category. Future of Privacy Forum, *supra* note 61.

(one-to-one). The risks posed by the use of facial recognition in these circumstances are unique, but likely the most readily understood by the public. Instances of facial recognition misidentifying individuals as crime suspects or other bad actors (potentially as a result of system bias) are well-publicized and cause understandable concern in many. There are other serious, albeit less dramatic, risks in the identification and verification contexts. For example, failed facial verification in the commercial context (say, boarding an airplane) could lead to individual frustration and delays in consummating important travel. Similarly, misidentification could cause a business to misattribute personal preferences, leading to unwanted—and irrelevant—advertising and targeted marketing. In the verification context, consent may be obtained initially as described above because an identity is necessarily associated with a facial template for verification to be possible. Nevertheless, either supplemental or more descriptive consent could be required for verification as it poses additional risks. One-to-one matching for verification, for example, could require “affirmative consent upon enrollment in a database.”⁷² Conversely, although one-to-many facial recognition, by definition, does not require assigning an identity to a facial template, the risks posed by misidentification are potentially serious. Again, affirmative, explicit, and prior consent may be most appropriate in these circumstances. One-to-one matching for identification could require “express, affirmative consent upon collection, prior to the matching process being initiated.”⁷³ As an additional protective measure, depending on other risk factors, such consent could be subject to “two-layer” consent, automatic expiration, or a requirement for affirmative consent each time an identification processing routine is performed.

2. *Adequate consent may vary by use.*

Although the stage at which facial recognition is being deployed may be a primary risk factor to consider when establishing consent requirements, the risks posed by specific use cases can, and often should, drive consent requirements. The drafting team will not consider the risks posed by every potential use case here; the list is long and growing. Some general use cases, however, can be instructive when considering the risks posed by facial recognition technology and how those risks may influence whether and which consent requirements are codified by legislators and policymakers.

Some use cases may pose relatively little risk. Consumer-level use of facial recognition for home security, depending on other risk factors, may not be particularly risky.⁷⁴ Assuming it is used for identification (not verification), the only required step would be the creation of a facial template, not the association of a template to an identity (except for those individuals requiring a reference

⁷² *Id.*

⁷³ *Id.*

⁷⁴ Such uses are not hypothetical. “Do-it-yourself” is readily available to consumers with modest investment of time, money, and skill. See Damen, “*Who can it be now? How to Build a Raspberry Pi Doorbell that Recognizes Friends*” (September 2021) available at <https://www.tomshardware.com/how-to/facial-recognition-doorbell-raspberry-pi>; Henriksen, *Interactive Face Recognition Application through Docker* (September 2021) available at <https://towardsdatascience.com/interactive-face-recognition-application-through-docker-85e86ad0ffa6>.

template). Risks associated with consumer-level use are mitigated by the lower likelihood that a consumer implementation would be targeted by data thieves; the data set would generally be too small to be worth the effort.⁷⁵ In this instance, mere notice and implied consent may be sufficient.

Conversely, high-risk uses such as those associating a facial template with an identity in sensitive circumstances may compel the most stringent consent requirements. For example, consider a telemedicine application that would require a facial verification prior to allowing the user to obtain medical care from a large medical practice or hospital system. As an initial matter, the risk here is heightened by the association with personal health information and, unlike the use discussed above, the health information might be a more attractive target for bad actors. Furthermore, a potential verification failure in this situation could result in delayed or denied medical care. The risks in such an implementation are particularly high and may justify a robust consent mechanism, such as requiring explicit, written, two-layer consent at each telemedicine session.

As the use cases for facial recognition develop, different risk matrices will take shape. Although legislators and policymakers cannot account for each potential use case, they should pay particular attention to those use cases posing the highest risk and consider subjecting them to the most stringent consent requirements, while allowing for the possibility of more relaxed requirements for lower risk uses.

3. *Secondary use and transfer may require heightened consent.*

Secondary uses of facial recognition data—uses other than those presented upon initial consent—may require subsequent, affirmative consent, especially where those uses are materially different than what was represented at the time of collection. In addition, any consent for potential future uses of facial recognition data in a way that deviates from the purpose for which the data was originally collected, may also require special consideration. In order to avoid situations where consent to future use becomes an unconditional license for all secondary uses, legislators and policymakers should consider whether entities should be required to disclose anticipated future uses with specificity, and only seek consent for those uses that are reasonably anticipated as opposed to those that are purely speculative. This is of particular importance when the collecting entity anticipates selling or sharing biometric data to another person or entity who could not otherwise be able to identify the individual.⁷⁶

In addition, consent to third-party transfers could require specific—not “all-or-nothing”—consent. Legislators and policymakers may want to consider whether collecting entities could allow individuals the choice to opt into the collection and use of data by the collecting entity for its primary purpose, while declining to allow any secondary use or transfer of data to a third party.

⁷⁵ This is not to say that consumer implementations should be exempted from any security requirements placed on facial recognition technology. See Section VII below.

⁷⁶ Future of Privacy Forum, *supra* note 61.

Such layered consent requirements would likely not apply to third-party vendors contracted by the entity to carry out the uses in the entity's original disclosure.

4. *Consent should be freely given and free from undue coercion or deception.*

Legislators and policymakers will also want to consider taking steps to ensure that any consent obtained is freely given. The individual consenting to the use of facial recognition technology should have an actual choice to make. This means that the choice should be voluntary, and that it should not be coerced or obtained through deception. Legislators and policymakers will want to be cognizant that there may be some scenarios in which the very nature of the relationship between the end user and the entity using facial recognition technology suggests that the choice to accept or decline the use of facial recognition technology is not voluntary. This may be the case in scenarios where the entity using the technology and asking for consent is in a position of power over the individual, for example a public sector entity, a medical care provider, or an employer. Such a power imbalance may lead the individual to believe that they have no choice but to agree, either because they depend on particular services or fear the consequences of saying no. This power imbalance is one of the reasons consent is not an appropriate vehicle for some public sector uses of facial recognition technology. In some instances, this concern could be allayed by making clear to the individual that there will not be any adverse consequences to refusing consent and ensuring that circumstances around the collection of consent do not place unfair pressure on that individual.

The drafting team uses the qualifier “undue” here because a wide array of factual circumstances may be considered “coercive” without negating consent because the individual still has meaningful choice. For example, a retail business may offer the consumer special discounts to consent to the use of facial recognition to track that consumer's reaction to products it sees on the store's shelves and send targeted advertising. It could be argued that merely offering a discount is coercive, although it might be more appropriate to view such a proposal as a mere incentive. In either event, the drafting team would generally not consider such an incentive undue coercion.

There may, however, be circumstances in which requiring consent to facial recognition technology in exchange for providing a service or product, where the use of the technology is not necessary for that service or product, could constitute undue coercion. For example, say that facial recognition is being deployed by a grocery store in a “food desert” and that consumers are induced to consent in exchange for discounts. Without the facial recognition incentive, the business may set above-market food prices. In that situation, the only way for the consumer to obtain “reasonable” food prices would be to consent to facial recognition given the consumer's lack of access to alternative venues. This implementation may be considered unduly coercive both because the consumer does not have any meaningful choice, and the products at issue are necessities. In this “take it or leave it” consent regime, individuals may feel that they are being pressured to make a choice they might not otherwise want to make in order to obtain the benefit of a particular product or service.

On the other end of the spectrum, prospective legislation could prohibit businesses from refusing to provide services where a consumer refuses to consent to facial recognition for non-security purposes such as marketing. The drafting team can foresee a middle ground, however, where entities that provide “essential” services or goods may be prohibited from refusing to condition the sale of essential goods and services on facial recognition consent but may condition enhanced services on consent. Essential services and goods might include, for example, food and beverage, lodging generally available to the public, housing and real estate, transportation-related goods and services, medical/dental/mental health services and products, public educational services, utilities, telecommunications-related goods and services (including ISPs), and ingress to public property where the public is commonly allowed (streets, parks, beaches).

Another scenario in which consent might not be freely given by an individual is when consent is obtained through the use of dark patterns, or other user interfaces or interactions that are manipulative or deceptive. Under circumstances in which a user interface/user experience is designed in a manner in which an individual is likely to be confused about the elections they are making, or how to effect the choices they wish to make (for example, the use of double negatives, opt-out slide bars with confusing or contradictory explanations, in which the title of the bar contradicts its explanation, or in which the default settings are inconsistent with a reasonable data subject’s expectations), there is no reason to believe that a data subject’s nominal “consent” as logged and asserted by the developer, corresponds to any actual volitional choice by the data subject.

5. *Consent should be freely revocable.*

Subject to reasonable technological limitations, legislators and policymakers will want to consider whether actual choice also requires providing an individual who has consented to the use of facial recognition the right to revoke their consent. Under circumstances in which an individual revokes their consent to the collecting entity’s use of the individual’s data (for example, the individual no longer does business with a company that used facial recognition for access control), honoring an individual’s decision to revoke their consent to the use of the data per se (in the form of the data subject’s gallery images and associated derived template/enrollment data) is likely to be fairly straightforward.⁷⁷ However, the “right to be forgotten” as embodied in the General Data Protection Regulation⁷⁸ and statutes such as California’s Consumer Privacy Act and Privacy Rights

⁷⁷ Although one can envision circumstances in which data subjects requesting deletion of their data from a facial recognition system gallery database may, ironically perhaps, be required to provide a photograph of themselves for scanning and ingestion/templating into the system so that the system administrators can find the users’ data in the system, or as part of the process authenticating the requestor.

⁷⁸ See generally GDPR Article 17, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e2606-1-1>.

Act⁷⁹ becomes more complicated given that, in general, the data corresponding to people already in a facial recognition system is very often used in part to further train a facial recognition system. Many commercial systems are used in situations in which data subjects are required to at least nominally consent to use of the system (in connection with taking a college entrance, university, or professional certification examination online, for example), and those also require the data subject's nominal consent to the use of their data in the improvement of the facial recognition system itself.

While the manner in which “live” human field data is used to train a deployed machine learning facial recognition system may vary, the drafting team broadly anticipates live data subject data may be used to train a system on an ongoing basis in at least two general ways. First, in a typical identification (one-to-many) or verification (one-to-one) facial recognition system, some number of false positives or false negatives will become apparent to the system operators.⁸⁰ Programmers can feed this information about false positives and false negatives back into the system to teach the system to improve its matching algorithm.

Second, live user data could be used to help train a facial recognition system by providing a system with both a data subject's photo ID, as well as hours of footage of video in which the data subject appears (both of which are available to the owners of certain online/remote testing systems both technically and as a matter of nominal consent). This data can be used to train the system to help conduct time-progression analysis (relative to the date the ID was issued), and the hours of video can be used to train for adjusting for a range of different camera angles and facial expressions (as the data subject moves during the video).

Society has been grappling with what the “right to forget” means in the context of situations where an individual's biometric information has been used to develop or improve a machine learning model or algorithm for some time. The matter is made complicated by the fact that the exact details of how a particular trained facial recognition AI algorithm (and those developed by machine learning systems such as artificial neural networks in particular) will generally not be entirely understood by the developers of the systems themselves. This lack of understanding ensues because the system itself made many of the determinations about how to evaluate the data to conduct the facial recognition task.

⁷⁹ Cal. Civ. Code s. 1798.105, https://leginfo.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.105.&nodeTreePath=8.4.45&lawCode=CIV as amended effective 1/1/2023, see https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

⁸⁰ E.g., as discussed above, a false negative for a verification system at a port of entry checkpoint is likely to become apparent almost immediately; but a false positive perhaps much later (after an audit of the system following a crime committed by the person who illegally entered the country, for example). In an identification (one-to-many) setting, the operator may be able to reject a false positive based on direct personal observation, or the false positive may become apparent later, after confirmation of an alibi of the person whose gallery image/template data the system matched to the query image.

However, while no image data of any particular data subject exists in a facial recognition algorithm *per se*, in the sense that any data subject's image or template data could be retrieved directly from the system model itself, it has been generally assumed by many that a fully-realized GDPR right of deletion may well include the right to undo the specific improvements to the facial recognition algorithm that were accomplished with the requesting data subject's data.⁸¹ This is despite the fact that neither the GDPR nor the various member supervisory authorities have provided any clarity around the question of whether the right to be forgotten includes the right to have the training impact of one's personal data eliminated from machine learning models, or the related question of whether a system owner may avoid a deletion request as to machine learning model training impact if it can establish the impossibility or impracticability of deleting the training impact of individual subjects' data.⁸² A supervisory authority arguing that the right of deletion is not subject to a technical feasibility refusal is likely to point to the fact that unlike other individual rights such as the data portability right,⁸³ the right of deletion under GDPR Article 17 contains no impossibility or proportionality test nor a general technical or cost feasibility test, except with respect to the controller's obligation to take reasonable steps to inform other controllers of the deletion request when the first controller has made the personal data public.⁸⁴ That being said, policymakers should be aware of the difficulty inherent in trying to "unring the bell" in these circumstances.

Regardless of the applicable law, researchers have shown that by repeatedly submitting randomly generated facial data as part of a model inversion attack, it is possible to recover at least low-resolution facial images of a specific person whose image data is known to have been used in model training. This is particularly true for those machine learning facial recognition systems that

⁸¹ This is based not on the direct extraction of a data subject's data in its original form from an AI model, but the more indirect derivation of some identifiable information about particular data subjects based on model inversion attacks that would permit a sufficiently motivated party with access to the system to derive some information about a particular data subject, in a manner broadly analogous to attacks on anonymized datasets in the area of differential privacy, *see, e.g.*, Graves, *et al.*, (2020) "Does AI Remember? Neural Networks and the Right to be Forgotten," (Draft) UWSpace. <http://hdl.handle.net/10012/15754>. Differential privacy and k-anonymity involve the application of statistical techniques such as the addition of noise, the reduction of data granularity, or the distribution of subject records within different datasets, in order to prevent an attacker from identifying composite individual data—if such privacy protection techniques are not applied, an attacker with sufficient motivation and resources could derive specific information about individuals from a composite dataset, and match that data with particular named people in the community, by making LSAT "puzzles and games" style matches and inferences on a massively complex, computer-aided scale. Li, et al. (2018) "Artificial Intelligence and the Right to be Forgotten," https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1816&context=faculty_scholarship).

⁸² Villaronga et al., (2018) "Humans Forget, Machines Remember," https://scholarship.law.bu.edu/faculty_scholarship/817/.

⁸³ *See* Article 14(5)(b) <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e2355-1-1>.

⁸⁴ Article 17(2) <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e2606-1-1>.

return a confidence measure with image query results, even when the recognition system in question does not contain the target data subject's actual facial images or enrolled templates in its gallery as such.⁸⁵ Countermeasures and protections, including those based on differential privacy and other privacy protection methods may address these vulnerabilities, and techniques are being developed to permit system owners to strip out or roll back the effects of individual subject data on an algorithm.⁸⁶

Because of the lack of consensus as to the scope of the right of deletion in the context of AI systems, barring the implementation of a strong anonymity solution with a firm basis in data science, we should continue to assume that, as a practical matter, the only current way to be sure that a single subject's data is securely removed from a recognition model is to retrain the entire algorithm from scratch, *i.e.*, as it existed prior to any training.⁸⁷ Given the massive amount of computer overhead typically involved in the ingesting and training process, there is a compelling case to be made by the developers of such systems that it is not technically feasible to retrain their systems every time they receive a deletion request from a data subject. Entities will therefore need to consider whether there are some circumstances in which individuals will not be able to revoke their consent. For example, entities could honor a revocation of consent for future uses of the data, but not for uses that have already occurred and where the personal data cannot reasonably be deleted without frustrating the purpose for which it was originally used.

D. Where providing notice and obtaining consent are not feasible, entities must take measures to ensure accountable use of facial recognition technology

There may be certain use cases where a notice and consent model is not appropriate because it would not adequately protect individuals from the various potential privacy and other harms potentially inflicted by the use of facial recognition technology. As described above in this commentary, situations where consent cannot reasonably be obtained from all individuals subject to the technology could include circumstances where national security considerations merit covert use of the technology by the government. Where that is the case, legislators and policymakers should

⁸⁵ Fredrikson, et al., (2015) "Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures," <https://www.cs.cmu.edu/~mfredrik/papers/fjr2015ccs.pdf>.

⁸⁶ Ginart, et al. (2020), "Making AI Forget You: Data Deletion in Machine Learning," <https://arxiv.org/pdf/1907.05012.pdf>, Bourtole, et al. (2020), "Machine Unlearning," <https://arxiv.org/pdf/1912.03817.pdf>, and *see generally* Fukuoka, et al., (2020) "Model Extraction Oriented Data Publishing with k-anonymity" at https://link.springer.com/chapter/10.1007%2F978-3-030-58208-1_13 (discussion of model inversion attacks, and privacy countermeasures for machine learning systems other than facial recognition systems).

⁸⁷ Tiffany Li, Eduard Fosch Villaronga & Peter Kieseberg, Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten, 34 Computer Law & Security Review 304 (2018); available at: https://scholarship.law.bu.edu/faculty_scholarship/817.

consider implementing measures to ensure that the entities deploying the technology are accountable. In the commentary to this principle below, we set forth a number of considerations relating to accountability wherein entities using facial recognition technology are operating outside of a notice and consent model. Although the considerations outlined below could be implemented in full, not all measures may be necessary to ensure adequate accountability given the particular circumstances at play. The goal, here, is less to prescribe a specific approach but to model a cohesive strategy that could be used by legislators and policymakers to ensure that such uses of facial recognition technology adequately mitigate the risks identified in Section V. This principle is designed to ensure sufficient transparency concerning how the technology is being used. This transparency is necessary to ensure that legislatures (and the public to which they are accountable) have a meaningful opportunity to evaluate and respond to the technology such that they can create fair but effective accountability surrounding its use in circumstances where notice and consent are not appropriate. The drafting team notes that even though the accountability measures outlined below are intended to provide additional protections where notice and consent are not feasible, even entities providing notice and obtaining consent to uses of facial recognition technology would benefit from consideration of issues discussed in this principle.

Moreover, it may be useful to understand these measures, especially those that create an opportunity for stakeholder review of a prospective plan of use, to constitute a form of implied or constructive consent by the affected community. In that way, the citizenry is provided notice of the intended use of facial recognition technology and, by normal legislative process, has an opportunity to reject the plan or, by inaction, to assent.

One way to ensure accountability is for entities to document their intended use of the technology and to provide some mechanism for stakeholder review of that plan. This would ensure that the legislatures and the public to which they are accountable have a meaningful opportunity to evaluate and respond to expected uses of facial recognition technology, and to invoke legislative and/or administrative processes where available. The plans for prospective use may be general enough to protect operational success and officer safety, but must still provide sufficient transparency for the public, legislators, and administrative arbiters to assess whether the conditions and manner of use are acceptable. Legislators and policymakers could have these plans address, for example:

- The permissible persistence and pervasiveness of surveillance.
- Whether the proposed use unjustifiably and broadly surveils without notice to those who are not the subject of criminal suspicion.
- Whether the use is generally consistent with Fourth Amendment jurisprudence applicable in the jurisdiction.
- Whether the proposed use is narrowly tailored to its objective.

- Whether the actions to be taken based on the surveillance properly reflect procedural and substantive due process.
- Whether a competent, unbiased, and transparent assessment indicates that technical performance of the system (including any data sets upon which it relies) meets defined standards for accuracy and the absence of bias.⁸⁸
- Whether the data set against which any matching is performed is constructed from permissible sources.
- Whether the imaging and extracted features are properly protected from misappropriation or other improper use.
- Whether constraints on the use of facial recognition technology prevent its use in a manner that may reasonably be expected to suppress exercise of the right of free speech or assembly, such as the development of dossiers of those not the subject of criminal suspicion, or unequal and harassing use in the prosecution of misdemeanors against those exercising constitutionally protected rights.
- Whether the conditions for use are defined and applied consistently according to specified neutral principles.
- Whether operators of the system are trained in proper usage of the system.
- Whether alternatives to the use of facial recognition technology are cost-prohibitive or impracticable.
- Whether law enforcement would be at a relative disadvantage in not using facial recognition.
- Whether unapproved secondary uses may be made of any information generated or collected through the deployment

One mechanism to ensure accountability and the creation of transparent and detailed plans would be for policymakers and legislators to adopt standards for such plans, which could draw from the elements outlined above. The particular standards adopted by policymakers and legislators would ultimately depend on the priorities and sensitivities of the community in which the technology would be deployed. Such standards could then guide entities in describing and justifying their planned use of the technology. Even absent such standards, however, legislators and policymakers may want to encourage entities within their jurisdiction to use the listed factors to evaluate and adjust planned uses of the technology so as to minimize public opposition to deployment of the technology and to ensure adequate protection of those subject to the technology. Careful consideration of the technical proficiency of the technology as planned for deployment may

⁸⁸ This assessment should be made using those who would actually operate the system so as to ensure that operator influence on the reliability of the system is evaluated. For purposes of this element, “competent, unbiased, and transparent assessment” means an evaluation against neutral performance standards for accuracy and neutrality (*i.e.*, the absence of bias), which standards apply according to the use(s) to which the facial recognition technology will be put such that the most stringent standards apply when the technology will be used as evidence of the identity of an individual who is or will be alleged in a court of law to have committed one or more felony crimes.

also help entities avoid successful challenges to admissibility of the resulting evidence and survive challenges framed around the constitutional principles described above in Section V. This transparency should also help ensure that entities can make investments in acquiring and developing the capacity to use facial recognition without concern that their planned use is one that the affected community is unwilling to tolerate. Such an approach would hopefully result in fewer viable legal challenges to uses of the technology and/or fewer demands for outright prohibition of the use of facial recognition technology. Prospective plans may also provide an opportunity for the research, development, and academic communities to identify needs and challenges that could be addressed by their work.

Another mechanism to ensure accountability could be submitting the general use plan for evaluation by a technically competent authority. Facial recognition technology may be technically competent for one use, say in developing a photo array, and not competent for another, say, perpetrator identification. And, as noted elsewhere in this document, particular instances of the technology can suffer from technical defects that result in bias and false positives. Courts may not be the ideal arbiters of the technical sufficiency of this technology, with judges and jurors potentially lacking the time, resources, and expertise for thorough evaluation. Thus, legislators and policymakers should consider ways to ensure that the particular software, datasets, and methodologies planned for use are carefully evaluated by an entity with technical competence to accurately assess the reliability of the planned approach. For example, an entity with the appropriate technical expertise could be empowered to evaluate the use of facial recognition technology by law enforcement to determine whether actual use is consistent with the relevant general use plan. That entity could document its evaluations and the basis for its findings of fact and make those findings available in a timely fashion to the general public. This evaluation could help the government overcome legal challenges to use of the evidence generated by the technology and guard against injustice.

Legislators and policymakers should also recognize that there may be novel or exigent need situations arising where the technology would be useful, and that were not anticipated by the entity in its prospective use plan. The aim of this element is to ensure that these exigent circumstance scenarios can be accommodated, but do not become an exception that swallows the rule or a means by which transparency is vitiated. Legislators and policymakers should consider when uses may be permissible even though they were not previously disclosed. This could be, for example, where:

- The use was not foreseen or foreseeable at the time the general use plan was offered for review;
- A good faith basis exists to believe that the use would be approved as part of a general use plan;
- The conditions and manner of each such individual use are offered for competent legislative and/or administrative review within 48 hours of deployment; and

- The use is reasonably calculated to deter, identify, and/or apprehend those engaged in activities that may constitute a felony.

Legislators and policymakers may also want to consider mechanisms to deter uses that are not consistent with the prospective use plan, and that, therefore, did not provide the public with constructive notice. One option could be holding individual law enforcement officers accountable for misuse of the technology. This would have the potential to deter violative conduct and, thereby, eliminate or minimize damage to specific cases and/or calls for legislative prohibition of use of the technology in law enforcement. Individual accountability could also promote attentive learning when law enforcement officers are trained in the proper use of the facial recognition technology on which they will rely. For example, one approach could be civil sanctions against the law enforcement officers who authorized or directed the deployment, with the potential for criminal sanctions where the uses were gross departures demonstrably made recklessly or in bad faith.

Finally, the mechanisms for accountability described above simply propose a framework by which entities can provide constructive notice to the community and would permit use of facial recognition technology to be evaluated on an ongoing basis. Although beyond the scope of this commentary, legislators and policymakers may also wish to consider whether there are evidentiary rules that would reduce some of the risks attendant to using facial recognition technology for law enforcement. For example, the drafting team discussed the potential for the following prohibitions:

- Evidence of facial geometry and associated imagery should never be the primary or sole evidence adduced in court of the identity of the perpetrator of a crime.
- When facial recognition technology has been used in the investigation of a crime, the fact and nature of that use must be presented to counsel for the defense at the same time and in the same manner as exculpatory evidence.
- Any time that evidence from facial recognition technology will be presented as evidence of the identity of the perpetrator of a crime, the government must permit counsel for the defense to review and evaluate the technical performance of the facial recognition technology and its manner of use in the case.
- No facial recognition evidence should be adduced in court as proof of identity where the defendant is among those that the technology deployed would confuse with a master face.

Whether or not they are feasible, such evidentiary rules would have the potential to serve as guardrails that allow legislators and policymakers to move forward with the use of facial recognition technology and insulate the technology from some of the criticisms that have arisen in certain contexts and that have resulted in bans or moratoria.

E. Face geometry data should be subject to data security standards appropriate to the risk

As explained above, the use of facial recognition technology comes with a high degree of risk. What happens when an individual's facial geometry or other biometric data is acquired by an unauthorized third party? The bad actor gains access to a highly trusted key that could open up access to the individual's financial accounts and devices. The risk of a data breach demonstrates the need to protect the underlying biometric data.

Moreover, unlike other types of sensitive personal information, it is difficult to remediate the potential damage caused by compromised biometric data. The Illinois legislature recognized this within the text of BIPA by stating:

Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.⁸⁹

Unfortunately, these risks are not merely hypothetical. Already there have already been several high-profile data breaches that have compromised individuals' biometric data. For example, in 2019, the U.S. Customs and Border Protection (CBP) disclosed a vendor data breach involving individuals' photographs and driver's license images that impacted approximately 100,000 individuals.⁹⁰ As a result of the incident, at least a portion of these individuals' data was offered for sale on the dark web.⁹¹ As indicated in a report on this incident by the Office of the Inspector General (OIG), since 2017 the Department of Homeland Security considers biometric information to be "sensitive personally identifiable information" (SPII) and thus afforded the highest level of security.⁹² The OIG's report found that the CBP, through its vendor, failed to comply with policies

⁸⁹ 740 Ill. Comp. Stat. Ann. 14/5(c). *See also* GAO Report, *Facial Recognition Technology - Commercial Uses, Privacy Issues, and Applicable Federal Law*, at 16 (July 2015) ("Because a person's face is unique, permanent (absent surgery), and therefore irrevocable, a breach involving data derived from or related to facial recognition technology may have more serious consequences than the breach of other information, such as passwords or credit card numbers, which can be changed.").

⁹⁰ Drew Harwell and Geoffrey Fowler, *U.S. Customs and Border Protection Says Photos of Travelers Were Taken in a Data Breach*, WASH. POST (June 10, 2019), available at <https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/>.

⁹¹ *Id.*

⁹² Office of Inspector General, *Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot* (Sept. 21, 2020), at 4.

and procedures in place to protect such SPII when the vendor downloaded the SPII onto its own network in an unencrypted state.⁹³

Despite these risks and the ever-increasing prevalence of both malicious and inadvertent data breaches, privacy and data security laws have been slow to account for biometric data. Even biometric-specific laws in Illinois, Texas, and Washington contain only general high-level security requirements for biometric data.⁹⁴ For example, BIPA requires entities in possession of biometric data to “store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry.”⁹⁵ The National Biometric Information Act of 2020, introduced in August of 2020 in congress, contains a similar flexible standard for protecting biometric data. In addition, an increasing number of state data breach notification laws include biometric information, or some derivation of that term, within the definition of triggering “personal information.”⁹⁶

However, the majority of states have few to no requirements or standards surrounding the protection of biometric data. This is true even in states with historically more stringent data security protections, such as Massachusetts. While Massachusetts is typically thought of as an outlier in that it requires companies processing certain types of personal information to implement a fulsome written information security program, the definition of “personal information” is narrow and does not cover biometric data, and the regulation of facial recognition technology is being pursued on a municipality-by-municipality basis.⁹⁷ With the approaching effective dates of the California Privacy Rights Act (CPRA), Virginia Consumer Data Protection Act (CDPA), and Colorado Privacy Act (CPA), each of which include biometric data within the definition of “personal information,” companies operating in those states will have at least a baseline requirement to maintain reasonable administrative, technical, and physical data security practices.

Given the size and economic importance of California, in addition to the other states discussed above, the standards set forth by the CPRA operate as a sort of *de facto* requirement for all national or international companies. However, there are still gaps in the many privacy and security laws in the United States that have the potential to leave biometric data without reasonable security controls. Given the potential risk of harm associated with the loss or misuse of an individual's

⁹³ *Id.*

⁹⁴ 740 Ill. Comp. Stat. Ann. 14/15(e)(1).

⁹⁵ S.4400, 116th Cong. (“A private entity in possession of a biometric identifier or biometric information shall store, transmit, and protect from disclosure all biometric identifiers and biometric information—(1) using the reasonable standard of care within the private entity's industry; and (2) 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.”).

⁹⁶ *See, e.g.*, Cal. Civ. Code § 1798.82(h)(1)(f) (“Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.”).

⁹⁷ *See* 201 CMR 17.00 et seq.

biometric data, these gaps should be closed and any entity collecting or using biometric data should be subject to sensible data security standards that are both commercially reasonable and appropriate to the risk.

The question then becomes what security controls are “reasonable and appropriate to the risk.”⁹⁸ As a starting point, biometric data, as a subset of personal information, should be subject to general reasonable security standards. Some variation of this standard is used throughout existing U.S. privacy laws and standards as evidenced by its use in the FTC’s “privacy by design” guidance and standards. Legislatures continue to use “reasonableness” as a standard in the next phase of U.S. privacy laws, such as the CCPA, CPRA, etc.

However, given the uniqueness of biometric data for the reasons set forth above, legislatures may choose to go above and beyond a generic reasonableness standard. Specific to biometric data, legislatures may also choose more detailed or proscriptive security controls. We outline four such controls below.

First, one of the most common security mechanisms available to protect facial geometries is to segregate any biometric data from other types of personally identifiable information.⁹⁹ Using this method, the data is stored as an encrypted digital template as opposed to a raw original image.¹⁰⁰ While the inherent identifying nature of biometric data would not render this data entirely secure or incapable of identifying an individual, this method creates a firewall that would require additional steps and analysis before being rendered in a usable state by a third party. Because “[e]ach developer measures and records [biometric] templates differently” this step provides “an additional layer of security by making this data useless if compromised, either for identification or as a credential outside of the system that created it.”¹⁰¹

Second and perhaps most obviously, given the highly sensitive nature of biometric data, facial geometries should be encrypted throughout the life cycle of the data, including both at rest and in motion.¹⁰² Best practices are developing which rely on new encryption technologies to protect the security of face representations including fully homomorphic encryption.

⁹⁸ See, e.g., FTC, Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission, June 13, 2020, available at (“[C]ompanies should employ reasonable security to protect consumer data.”).

⁹⁹ GAO, Facial Recognition Technology - Commercial Uses, Privacy Issues, and Applicable Federal Law at 25 (July 2015).

¹⁰⁰ Note that, even in this context, the underlying image should be adequately protected as well. See FTC, Best Practices for Common Uses of Facial Recognition Technologies at 12 (October 2012).

¹⁰¹ Security Industry Association, SIA Principles for the Responsible and Effective Use of Facial Recognition Technology (August 2020) available at <https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/>.

¹⁰² See, e.g., International Biometrics & Identification Association, Principles for Biometric Data Security and Privacy at 6 (August 2019).

Third, the common privacy principles of data minimization and purpose limitation may be applied specifically to the facial recognition context. Given the highly sensitive nature of biometric data, legislatures may wish to consider specific requirements and timelines governing data retention. For example, the Council of Europe’s Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data recommends that:

[E]ntities . . . have to ensure that different storage limitation periods apply to the different phases of the processing:

- if there is no match of the biometric templates, the biometric template of individuals passing through an uncontrolled environment cannot be retained and have to be automatically deleted;
- if there is a match, the biometric templates can be retained for a strictly limited time provided by law with necessary safeguards and match reports including personal data can also be retained for a limited time;
- and in any case, the watchlist and biometric templates have to be deleted upon completion of the purpose for which live facial recognition technologies were deployed.¹⁰³

While the ultimate standard needs to be flexible enough to account for various contexts and fact patterns, the overarching goal is to limit the amount of biometric data stored—and therefore potentially at risk—by entities.¹⁰⁴

Fourth and finally, an alternative option is found in BIPA, which does not use a tiered approach, but requires the development of “a written policy . . . establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.”¹⁰⁵ This written policy requirement could be expanded to include a written information security program targeted to protect facial recognition data.

¹⁰³ Guidelines on Facial Recognition (January 28, 2021).

¹⁰⁴ See also GAO, Facial Recognition Technology - Commercial Uses, Privacy Issues, and Applicable Federal Law at 24 (July 2015) (“Among the best practices recommended for companies using facial recognition technology were . . . implementing a specified retention period for personal data and disposing of stored images once they are no longer necessary for the purpose for which they were collected.”).

¹⁰⁵ 740 Ill. Comp. Stat. Ann. 14/15(a).

Appendix A:

City or County Level Ordinances

- **Arizona Data Security Breaches Law**

- In 2018, Arizona passed the Arizona Data Security Breaches Law. ARIZ. REV. STAT. ANN. § 18-551. Similar to the CCPA, the statute defines protected personal information as an individual's first name or initial and last name in combination with any specified data element, which includes unique biometric data. The law imposes notification requirements on persons conducting business who maintain unencrypted and unredacted personal information who become aware of security breaches. ARIZ. REV. STAT. ANN. § 18-552. The law does not provide a consent requirement nor a private right of action, but imposes a civil penalty, to be enforced by the Attorney General, of up to \$10,000 per affected individual.
- Covers FRT but also other forms of biometric information.

- **Arkansas House Bill 1943**

- In April 2019, Arkansas passed House Bill 1943, which revised Arkansas Code § 4-110-103(7) to include biometric data in the definition of "personal information." ARK. CODE ANN. § 4-110-103(7)(E). Revisions to the prior bill added a notification requirement to the Attorney General in the event of a data breach where more than 1,000 individuals have their personal information affected.
- Covers FRT but also fingerprints, faceprints, retinal and iris scans, hand geometry, voiceprint analysis, DNA, or any other unique biological characteristic of a person used to access a system or account.

- **California Assembly Bill 1215**

- Imposes a 3-year moratorium on use of FRT in police body cameras. Went into effect in January 2020. Authorizes a person to bring an action for equitable or declaratory relief against a law enforcement agency or officer who violates that prohibition.

- **Illinois Biometric Privacy Act (BIPA)**

- Enacted in 2008 to protect the privacy of personal biometric data. Section 15(a) of BIPA requires a company to publicly post a general notice about the company's biometric data retention periods. 740 Ill. Comp. Stat. 14/15(a).
- Section 15(b) of BIPA requires a company to provide specific notice and obtain consent from the particular person whose biometric information is collected. *Id.* at 14/15(b). BIPA also bans the sale or trade of personal biometric information for profit. *Id.* at 14/15(c).
- BIPA provides for a private right of action for anyone "aggrieved by a violation" of the statute. *Id.* at 14/20.
- 4. Covers FRT but also other forms of biometric information.

- **Louisiana Database Security Breach Notification Law**
 - Amended in 2018 by Senate Bill 361 to include biometric data under the umbrella of data elements, which when combined with the first name or initial and last name of a state resident, constitute “personal information.” LA. STAT. ANN. § 51:3073. The statute provides the opportunity for an individual to recover actual damages through a civil action “resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person’s personal information.” Liability is strictly for actual damages from failure to timely notify.
 - Covers FRT but also other forms of biometric information.
- **Maine “Act to Increase Privacy and Security by Regulating the Use of Facial Surveillance Systems by Departments, Public Employees and Public Officials”**
 - **LD 1585.** State, county, and municipal governments, including schools, are not allowed to use or possess any sort of FRT, and may not enter into a third-party agreement to obtain, access or use FRT. Law enforcement may use the technology for investigating certain serious crimes, but state law enforcement agencies are barred from implementing their own FRT systems. They may request FRT searches from the FBI and the state Bureau of Motor vehicles in certain cases. The law stipulates any unlawfully obtained data must be deleted and is inadmissible as evidence, and that the results of a facial recognition search are not sufficient, without other evidence, to justify “arrest, search or seizure.”
 - Act also gives “injured or aggrieved” individuals the opportunity to seek “injunctive or declaratory relief” against a “department, public employee or public official” believed to be in violation of the law. A public employee or official who violates the law “may be subject to disciplinary action, including, but not limited to, retraining, suspension or termination,” the bill states.
 - Passed unanimously and will go into effect October 1, 2021.
- **New Hampshire**
 - New Hampshire bans police from using FRT on body cam footage, effective January 1, 2017: “Except as authorized in this section, no person, including without limitation officers and their supervisors, shall edit, alter, erase, delete, duplicate, copy, subject to automated analysis or analytics of any kind, including but not limited to facial recognition technology, share, display, or otherwise distribute in any manner any BWC recordings or portions thereof. This paragraph shall not apply to the sharing of a still image captured by the BWC to help identify individuals or vehicles suspected of being involved in a crime.”
- **New York SHIELD Act**
 - On July 25, 2019, New York adopted the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), ch. 117, 2019 N.Y. ALS 117. The SHIELD Act included biometric information in the definition of “private information,” imposes

security requirements for companies doing business in New York and notification requirements in the event of a breach. The SHIELD Act does not have a consent requirement nor a private right of action.

- Covers FRT but also other forms of biometric information.

- **Oregon Laws.**

- **Consumer Information Protection Act.** Effective January 1, 2020, adds to its definition of personal information “data from automatic measurements of a consumer’s physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer’s identity in the course of a financial transaction or other transaction.” OR. REV. STAT. § 646A.602 (2020). Unlike Arizona’s definition, however, this is not applicable if encryption, redaction, or other methods have rendered the data elements unusable, unless the encryption key has been acquired. *Id.* Like most other states, Oregon does not provide a private right of action. Covers FRT but also other forms of biometric information.
- **ORS 133.741** bans the use of FRT in police body cameras. Requires law enforcement agencies to establish policies and procedures that “prohibit the use of facial recognition or other biometric matching technology to analyze recordings obtained through the use of the camera.”

- **Texas Business and Commerce Code § 503.001**

- Effective September 1, 2017, and covers the capture or use of biometric identifiers. TEX. BUS. & COM. CODE ANN. § 503.001. Like the BIPA, Texas requires companies to not only inform the individual before capturing their biometric information, but also to obtain their consent. Consent must also be obtained for a possessor of biometric information to sell, lease, or disclose that information. *Id.* Further, possessors of biometric identifiers must destroy them within one year unless collected for a document required by another law to be maintained. Texas’s law provides no private right of action but imposes liability for a civil penalty of up to \$25,000 for each violation, to be brought by the Attorney General.
- Covers FRT but also other forms of biometric information.

- **Vermont S. 124**

- Bans police use of facial recognition technology statewide and prohibits police from using facial recognition technology without the express consent of the legislature. Law enforcement are permitted to use facial recognition in connection with data collection by law enforcement drones but only with respect to the specific target of the surveillance.
- Enacted 2020; modified in May 2021 in H.195 to carve out use of FRT in criminal investigations of sexual exploitation of children.

- **Virginia HB 2031**

- Provides that no local law enforcement agency or campus police department shall purchase or deploy facial recognition technology, defined in the bill, unless such

purchase or deployment is expressly authorized by statute. The bill prohibits a local law enforcement agency or campus police department at a public institution of higher education currently using facial recognition technology from continuing to use such technology without such authorization after July 1, 2021.

- **Washington House Bill 1493**

- In May 2017, Washington State enacted House Bill 1493, which added protections for consumers' biometric information. Codified at WASH. REV. CODE ANN. § 19.375.020, the law imposed a consent requirement for the collection and commercial use of biometric information, and set a reasonable care standard for possessors to guard against unauthorized access and limited retention of the information. Washington later amended a separate statute on notice for security breaches to include biometric information as "personal information." 2019 WASH. H.B.1071. The statute requires notice within 30 days in the event of a security breach when it is reasonably likely to subject consumers to a risk of harm or if the confidential process or encryption key was acquired by an unauthorized person, and provides that any consumer injured by a violation of the statute may institute a civil action to recover damages.
- Covers FRT but also other forms of biometric information.

City or County Level Ordinances

- **California**

- **City of Alameda.** The City Council of Alameda, CA banned the use of FRT by city agencies, including police, in December 2019. The Ordinance has a carve-out for situations where outside agencies seek help from Alameda police. At that time, the council also directed staff to formulate a more binding city ordinance to ban the future use of facial-recognition technology in Alameda, along with a data management and privacy oversight ordinance. There has been some reporting that law enforcement in Alameda is using FRT with Clearview anyways.
- **City of Berkeley.** The City Council of Berkeley, CA banned the use of FRT by city agencies, including police, in October 2019. The Ordinance also requires council approval for purchase of FRT.
- **City of Oakland.** In July 2019, the City Council of Oakland, CA banned the use of facial recognition technology by city agencies, including the police department. The Oakland ordinance also includes whistleblower protections and a prohibition on non-disclosure agreements.
- **City of San Francisco.** In May 2019, banned use by government agencies and law enforcement. The ban prohibits city agencies from using facial recognition technology, or information gleaned from external systems that use the technology. It is part of a larger legislative package devised to govern the use of surveillance

technologies in the city that requires local agencies to create policies controlling their use of these tools. There are some exemptions, including one that would give prosecutors a way out if the transparency requirements might interfere with their investigations.

- **Louisiana**

- **City of New Orleans.** The New Orleans City Council passed a ban on four pieces of technology—facial recognition, characteristic recognition and tracking software, predictive policing and cell-site simulators in December 2020, which holds city officials and entities cannot “obtain, retain, possess, access, sell, or use any prohibited surveillance technology or information derived from a prohibited surveillance technology.” Allows city to use evidence derived from facial recognition or characteristic tracking software “so long as such evidence was not generated by, with the knowledge of, or at the request of the City or any City official.”

- **Maine**

- **City of Portland.** City council enacted a preliminary ban on use of FRT by city employees in August 2020. Voters in November 2020 enacted a stronger ban on use of FRT by government employees by ballot initiative, which includes a private right of action and entitlement to \$1,000 in fines. The city does not currently use FRT. This seems to go farther than the recently enacted Maine statute.

- **Massachusetts**

- **City of Boston. Ordinance #0683** was passed by the Boston City Council in June 2020. Prohibits use of FRT by city and city employees and prohibits city and city employees from entering into third-party agreements to purchase or use FRT. Authorizes private right of action and attorney’s fees if violated.
- **City of Brookline.** Brookline voted to ban facial recognition technology use by government or government employees at their town meeting 179-8 in December 2019.
- **City of Cambridge.** The Cambridge City Council voted to prohibit city departments from accessing or using facial recognition technology and information obtained from the software in January 2020.
- **City of Northampton.** The Northampton City Council voted to prohibit Northampton from collecting and using people’s biometric information through surveillance technology in December 2019.
- **City of Somerville.** In June 2019, the City Council of Somerville, MA banned the use of facial recognition technology by city agencies, including the police department. Includes a private right of action and attorney’s fees if violated.
- **City of Springfield.** In February 2020, the City Council of Springfield, MA restricted the municipal use of facial recognition technology until the city’s police department puts forward rules governing the software that the council then approves.

- **Minnesota**
 - **City of Minneapolis.** In February 2021, Minneapolis City Council voted to ban use of FRT by the Minneapolis Police Department. The ordinance includes an appeals process allowing city agencies to request exemptions under some circumstances.
- **Mississippi**
 - **City of Jackson.** In August 2020, the Jackson City Council voted to preemptively ban the Jackson Police Department from using facial recognition technology to identify people.
- **Oregon**
 - **City of Portland.** Portland’s FRT ban, enacted in September 2020, prohibits not just government FRT use but also many applications of facial recognition by private companies. Was passed as two ordinances. The first ordinance bans the use and acquisition of face recognition technologies by City bureaus—went into effect immediately, and applied to all City of Portland bureaus and offices. The second ordinance went into effect January 1, 2021, and banned private entities from using facial recognition technology in places of public accommodation and included all private entities in Portland.
- **Pennsylvania**
 - **City of Pittsburgh.** The City of Pittsburgh City Council voted in September 2020 to regulate the use of facial recognition and predictive policing technologies by city entities, including the Pittsburgh Bureau of Police. The legislation requires city council approval of such technologies before they are acquired or used, except in “an emergency situation.”
- **Washington**
 - **King County, Washington.** King County, Washington, which includes 2.3 million people in and around Seattle, passed an ordinance banning the use of FRT in June 2021.
- **Wisconsin**
 - **City of Madison.** In December 2020, Madison city council voted to ban use of FRT by government. Is considered a “partial ban” because it has a number of exemptions: the technology can be used to identify and/or locate individuals who are victims of human trafficking or missing children, can be used in electronic devices, such as a cell phone or tablet, that perform face surveillance for the sole purpose of user authentication, and can use automated redaction software, provided that it does not have the capability of performing face surveillance.

Appendix B

- The [Facial Recognition and Biometric Technology Moratorium Act of 2021](#) (S.2052 - 117th Congress) would make it unlawful for a federal agency or official to acquire, possess, access, or use a “biometric surveillance system” or information derived from such a system that is operated by another entity. The bill defines biometric surveillance system to mean “any computer software that performs facial recognition or other remote biometric recognition in real time or on a recording or photograph.” There is an exception to this broad prohibition for federal laws that set parameters around the use of such systems. Those laws must describe the entities permitted to use the biometric surveillance system, the purposes of such use, and any prohibited uses. They must also describe standards for the use and management of information derived from the biometric surveillance system, including data retention, sharing, access and audit trails. The bill also envisions that such laws would include auditing requirements to ensure the accuracy of biometric surveillance system technologies, standards for minimum accuracy rates, and accuracy rates by gender, skin color, and age, as well as rigorous protections for due process, privacy, free speech and association, and racial, gender, and religious equity.

The federal moratorium bill also makes any information obtained in violation of the bill inadmissible by the federal government in any criminal, civil, administrative, or other investigation or proceeding. Individuals injured by a violation of the act are provided with a cause of action against the federal government and can recover damages, attorneys’ fees and costs, and other relief. The act is also enforceable by the attorney general. Federal officials that have violated the act may also be penalized. In addition, the proposed federal moratorium would prohibit federal law enforcement agencies from using federal funds to purchase biometric surveillance systems, and makes it so that state or local governments will not be eligible to receive federal financial assistance under the Byrne grant program unless the state or local government is complying with a law or policy that is substantially similar to what the law envisions for a federal comprehensive law.

- The [George Floyd Justice in Policing Act](#) (H.R.1280 - 117th Congress), would ban the use of facial recognition technology in police body cameras and in-car video recording cameras in patrol cars. In addition, footage from those cameras or recording devices could not be subjected to facial recognition technology. The bill would also direct a study on issues relating to the constitutional rights of individuals on whom facial recognition technology is used as well as limitations on the use of facial recognition technology.

- The [Fourth Amendment is not for Sale Act](#) (S.1265 - 117th Congress), although not directly related to facial recognition technology, would require the government to get a court order to force data brokers to disclose data. It would also prohibit law enforcement and intelligence agencies from buying data about people if the data was obtained from a user's account or device, or through deception, hacking, violations of a contract, privacy policy, or terms of service. One of the stated motivations for the bill was Clearview AI's ability to compile its database of billions of photos, which it downloaded in bulk from consumer facing websites in violation of those websites' terms of service.