

The Sedona Conference Draft Commentary on Notice and Consent Principles for Facial Recognition Technology (April 2022)



The Sedona Conference Draft Commentary on Notice and Consent Principles for Facial Recognition Technology (April 2022)

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)

The Sedona Conference Commentary on Notice and Consent Principles for Facial Recognition Technology

April 2022
Draft Version

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	7
V. RISKS OF FACIAL RECOGNITION TECHNOLOGY	11
A. Risks to Individuals	11
B. Challenges to Businesses	13
VI. PRINCIPLES	15
A. A notice and consent framework alone offers insufficient protections for certain uses of facial recognition technology by the public sector.....	15
B. If a data subject's consent can be freely given, a notice and consent regime may be appropriate for government uses of facial recognition.....	17
C. Actual notice should be meaningful and transparent.....	18
1. Timing of Notice.....	19
2. Presentation of Notice	19
3. Content of Notice	20
D. Individual consent should be informed and express.....	21
1. Timing of Consent.....	21
2. Consent should be informed.....	22
3. Consent should be express	22
4. Consent should be freely given and free from undue coercion or deception.....	23
5. Secondary use and transfer should require additional consent	24
6. Consent should be freely revocable	25
E. Entities must take measures to ensure accountable and transparent use of facial recognition technology, especially where providing notice and obtaining consent are not feasible.....	27

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 technology improves and the corresponding data in the cloud continues to grow, both 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 the unique risks posed by this technology, there is currently no uniform statutory or regulatory regime governing its use in the United States, though there are some federal privacy laws that are applicable to the use of facial recognition technology depending on the circumstance.¹ This landscape, coupled with concerns expressed by some over the potentially problematic uses of this technology 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 attempts to bridge the divide between the moratoriums on the use of facial recognition technology and a comprehensive law regulating facial recognition technology, by recommending a framework that could form the underpinnings of such a law. We have not attempted to craft overall privacy principles, or specific legislation, for the use of facial recognition technology. Rather, in this Commentary we propose a set of 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.² Specifically, we explore whether a notice and consent model—which has been the prevalent model for U.S. privacy laws³—is appropriate given the unique concerns posed by facial recognition technology that may make

¹ See, e.g., Privacy Act of 1974, Public Law No. 93-579, as amended, codified at 5 U.S.C. § 552a.

² 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. See Robert H. Sloan and Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, J. HIGH TECH. L., 148, at 373-74 (2013). 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). https://scholarship.kentlaw.iit.edu/fac_schol/568?utm_source=scholarship.kentlaw.iit.edu%2Ffac_schol%2F568&utm_medium=PDF&utm_campaign=PDFCoverPages.

³ While there are limitations inherent in a notice-and-consent approach, it is a significant component of the fair information practice principles that have formed the basis for much U.S. law, including the Privacy Act of 1974, and privacy enforcement by the FTC under the FTC Act. See, e.g., “The Near Future of U.S. Privacy Law (Remarks of FTC Commissioner Slaughter) September 6, 2019, https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf.

reliance on a notice and consent model problematic in certain circumstances—particularly with respect to the public sector.

Section II of the Commentary provides a basic overview of how facial recognition technology works,⁴ while Section III provides examples of common uses of the technology. Section IV describes how the technology is currently regulated in the United States, and Section V analyzes the potential risks posed by the use of facial recognition technology, including risks to individuals and specific challenges faced by businesses. Finally, Section VI encompasses a series of guidelines that provide legislators and policymakers with suggestions on when a notice and consent framework may be appropriate for facial recognition applications, as well as what is likely to constitute adequate notice and consent. This section also offers recommendations for legislators and policymakers on an implementation governance model that could help ensure accountability and transparency for any proposed new uses of facial recognition technology.

As discussed in further detail throughout this draft Commentary, while facial recognition technology when used by the private sector as well as by government each pose risks to both individual and collective autonomy, the public sector's unique position of authority and its coercive power creates certain scenarios where consent cannot be meaningfully obtained. In the instances where the public sector cannot provide meaningful informed and freely-granted consent for the use of facial recognition technology, accountability and transparency will have to be achieved on a less granular basis. The drafting team did determine that there are uses of facial recognition technology where a notice and consent framework are appropriate given the intended use and relationship of the parties. This does not mean that private sector use cases and some public sector use cases are without risk, but rather that we determined that a notice and consent framework apparently provided sufficient guardrails for the uses of the technology. In the instances in which a notice and consent model are appropriate, the drafting team provides guidance for legislators and policymakers on what constitutes adequate notice and consent for the use of notice and consent when using facial recognition technology.⁵

Given the breadth of the topic, we have not attempted to comprehensively address the legal implications of the use of facial recognition technology. We only address 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 gaze tracking),⁶ or facial detection (determining whether a human face is

⁴ This basic overview of facial recognition technology is intended to provide sufficient context for readers of this Commentary to understand the issues discussed in this Commentary. The Sedona Working Group 11 Biometrics Primer provides a more comprehensive overview of biometric technologies generally, including facial recognition technology.

⁵ The primary intended audience for this commentary is state and federal legislators in the United States and other policymakers who 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 library of principals or best practices regarding the use and implementation of facial recognition technology.

⁶ 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).

present in an image at all) standing alone. We also do not address biometric technologies other than facial recognition technology. Although many of these principles may be relevant for policymakers and legislators focused on other biometric technologies, the unique circumstances of facial recognition technology may necessitate heightened protections. Finally, this commentary also does not address considerations around notice and consent as they apply to minors or individuals with diminished capacity, as greater protections for those individuals may be needed.

II. HOW FACIAL RECOGNITION TECHNOLOGY WORKS

Facial recognition technology is a type of biometric technology.⁷ Biometric technologies can be used to identify individuals based on one or more unique physical or behavioral characteristics. These characteristics can be relatively static, such as a fingerprint or face; or dynamic, such as how a person types, speaks, or walks.⁸ In the broadest sense, facial recognition technology describes a computer system that can recognize, or match, images of faces; it 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. 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:⁹

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).¹⁰

⁷ See, generally, The Sedona Working Group 11 Biometrics Primer (2022).

⁸ 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.

⁹ 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.

¹⁰ In this commentary, the drafting team refers to the image the user presents to the system at the point of use as the “query” image, although this input image is also frequently referred to in the literature as the “probe” image. See U.S. Government Accountability Office Report, *Facial Recognition Technology: Current and Planned Uses by Federal Agencies*, GAO-21-526, at 3 (August 2021).

Step 2 (Facial Template Creation). The first step in this process is facial detection—where the system determines whether 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.¹¹ After the system detects a face, 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 use these numerical data sets to quickly compare the data from one face against other facial templates.

Step 3 (Facial Template Matching). For any number of reasons, the system’s user may want to determine whether the particular person captured in the query image may be the same person depicted in an existing image¹² 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.

Users can compare the query image against one, or many, images from the gallery database, depending on the user’s goal.¹³

- **One-to-one matching (verification).** The user asks the facial recognition system whether the query image matches a particular single image from the gallery database.¹⁴

¹¹ 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.

¹² 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 corresponding photographic images as opposed to simply derivative numerical template data.

¹³ 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.

¹⁴ 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

- **One-to-many matching (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.¹⁵

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.

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 person¹⁶), 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

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.

¹⁵ 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.

¹⁶ 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.

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 and constitutes a unique risk in the widespread adoption of the technology.¹⁷

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 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 is a non-exhaustive list of several typical current, emerging, and potential applications of facial recognition technology, that may be considered with respect to notice and consent requirements.

- ***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.¹⁸
- ***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 person of interest within a crowd at a concert or sporting event.
- ***Private investigations.*** 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.*** In both the private and public sector, facial recognition technology may be used to control access to electronic devices and physical spaces.¹⁹ Facial recognition technology may also be used to verify the identity of travelers at

¹⁷ See *infra* Section V.A.

¹⁸ Though not the subject of this commentary, law enforcement may also use facial detection and facial recognition software to direct investigators to moments in voluminous, recorded surveillance video that contain faces, the same face seen elsewhere in the video(s), the face of a target of the investigation, or faces not found in a set of query images (*i.e.*, faces of people not expected or not authorized to be in the location surveilled).

¹⁹ A familiar example is the use of facial recognition technology to unlock a smartphone or to log in to a camera-enabled computer.

airports, and to authenticate the identity of employees entering a secure location in an office or factory.

- ***“Touchless” transactions.*** For commercial transactions, 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 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.²⁰ 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 and regulations²¹ that could apply to public sector or private sector uses of facial recognition technology depending on the particular circumstances:²²

- **Privacy Act**
- **State data breach notice laws**
- **State biometric privacy laws**

²⁰ 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.

²¹ The United States Government collects and uses biometric data for many purposes, including detecting and preventing illegal entry into the U.S., granting and administering proper immigration benefits, vetting and credentialing, facilitating legitimate travel and trade, enforcing federal laws, and enabling verification for visa applications to the US. The Department of Homeland Security provides biometric identification services to protect the nation through its Office of Biometric Identity Management whose mission is to uphold the privacy of people while protecting its borders, and its privacy practices are available at dhs.gov.

²² An overview of some of the laws and ordinances identified and surveyed by the drafting team can be found at Appendix A.

- **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 of biometric information. Additionally, a small subset of states have 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 aimed at facial recognition technology at all, but rather, attempts to fold facial recognition technology into the broader set of biometric information already regulated by the state, which may not address all of the unique concerns attendant to the technology. The California Consumer Privacy Act (“CCPA”)²³ 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 inclusion of unique biometric data in the scope of the protected information can be read to encompass facial recognition technology as well as other forms of biometric information. 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 it imposes civil penalties in the case of a breach but not a private right of action. Arizona, Arkansas, Louisiana, New York, Oregon, and Washington have data breach notice laws with similar approaches.²⁴

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 Information 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.²⁵ BIPA also requires a company to provide specific notice and obtain consent from the particular person whose biometric data is collected,²⁶ and bans the sale or trade of personal biometric data for profit.²⁷ BIPA provides for a private right of action for anyone “aggrieved by a violation” of the statute.²⁸ The Texas Business and Commerce Code § 503.001 bans the use of biometric data for commercial purposes without

²³ Cal. Civ. Code §§ 1798.110, *et seq.* The California Privacy Rights Act of 2020, which becomes effective in 2023, will revise and expand on the CCPA.

²⁴ The Louisiana and Washington laws include a private right of action for a failure to timely notify in the event of a data breach.

²⁵ 740 Ill. Comp. Stat. 14/15(a).

²⁶ *Id.* at 14/15(b).

²⁷ *Id.* at 14/15(c).

²⁸ *Id.* at 14/20.

prior notice and consent, and 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.

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 Federal Bureau of Investigation and the state Bureau of Motor vehicles in certain cases.

Additionally, the Maine 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.²⁹ 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 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

²⁹ The California moratorium went into effect January 2020.

are acquired or used, except in “an emergency situation.” New Orleans 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.”³⁰ The Portland, Oregon, ban contains a private right of action, with statutory damages of \$1,000 per day.³¹ 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.”³²

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.

Finally, although not laws or regulations, a number of organizations have developed best practices and general principles for using facial recognition technology. As part of its analysis, the drafting team surveyed these materials to understand existing guidance in this area and how these principles approach notice and consent. Many of the principles the drafting team 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. A description of some of the principles that the drafting team considered can be found in Appendix C.

³⁰ Portland, OR., City Code Ch. 34.10 (2020).

³¹ *Id.*

³² *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 use facial recognition technology.

A. Risks to Individuals

- **Overarching 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.³³ 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.³⁴ 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 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.
- **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

³³ See FTC Staff Report, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, at 7-8 (2012) (citing concerns of commenters).

³⁴ 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).

this technology ever violates a person’s “reasonable expectation of privacy” under the Fourth Amendment.³⁵

- **First Amendment Concerns.** Facial recognition systems can (and have been) deployed on 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.³⁶
- **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 a biometric gallery database is skewed, if a biometric algorithm is badly biased, or if biometric match parameters are insufficiently tight, the use of facial recognition technology may be “so impermissibly suggestive as to give rise to a very substantial likelihood of irreparable misidentification.”³⁷ 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 of a crime. In this way, an algorithm trained on 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.³⁸ 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.”³⁹ 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.⁴⁰ Among other issues, many commonly used datasets contain imbalanced demographic distributions that result in biased discrimination

³⁵ *Katz v. U.S.*, 389 U.S. 347, 361 (1967).

³⁶ 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).

³⁷ See *Simmons v. United States*, 390 U.S. 377, 384 (1968).

³⁸ See Larry Hardesty, *Study Finds Gender and Skin-Type Bias in Commercial Artificial Intelligence Systems*, MIT News Office, (Feb. 11, 2018).

³⁹ Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use*, WASHINGTON POST (Dec. 19, 2019).

⁴⁰ 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).

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.⁴¹ 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.⁴² 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 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. Additionally, most biometric-related laws do not include a private right of action, and thus are enforced by the relevant government regulator. When developing and/or deploying facial recognition technology, companies must consider which laws apply to their proposed use case(s) and implement appropriate compliance programs. An understanding of enforcement priorities, past and current investigations, and enforcement actions should also inform the company's approach to deploying facial recognition technology solutions.⁴³
- **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

⁴¹ Harwell, *supra* note 34.

⁴² 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.

⁴³ 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. 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." *In the Matter of Everalbum, Inc.*, File No. 1923172 (FTC Jan. 11, 2021).

suggestions” feature.⁴⁴ Facebook eventually settled this case for a landmark \$650 million.⁴⁵ 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 expected.⁴⁶ 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.⁴⁷ 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.⁴⁸ In less controlled settings, such as when there is bad lighting or where faces may be obstructed, the likelihood of misidentification increases.⁴⁹ 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.⁵⁰
- **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 of biometric data can present significant risk of harm to individuals. In addition to the loss of facial recognition data, unauthorized access to biometric data 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

⁴⁴ *In re Facebook*, 2018 U.S. Dist. LEXIS 81044, at *3.

⁴⁵ 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/>.

⁴⁶ 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->.

⁴⁷ *Id.*

⁴⁸ 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>.

⁴⁹ *Id.*

⁵⁰ See, e.g., K. Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, NY TIMES (Dec. 29, 2020).

adequately protect biometric data.⁵¹ Entities interested in using facial recognition technology 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. PRINCIPLES

- A. A notice and consent framework alone offers insufficient protections for certain uses of facial recognition technology by the public sector

An overarching concern with facial recognition technology is the potential for its use to infringe on an individual's privacy or our collective autonomy in a way that may not be present with other technologies. This concern is heightened for public sector actors that may not be similarly situated to private actors in many of their actions, positions, and coercive power, which calls into question whether there are certain uses of facial recognition technology in which the public sector cannot provide meaningful notice and obtain informed consent. The drafting team concluded that there were two scenarios in which public sector use of facial recognition technology were incompatible with a pure notice and consent framework. First, where the activity may infringe on a fundamental constitutional right—such as in the law enforcement or national security contexts—and, second, where the coercive relationship between the individual and the government taints the ability of a government to ever obtain freely given consent from an individual. In these circumstances, the relevant question for legislators and policymakers is 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.

Law enforcement is the most obvious example of a scenario in which the government's relationship to the individual calls into question Constitutional concerns as well as whether consent can ever be freely given. Law enforcement agencies have investigative and coercive powers that put them in a position of authority over individuals. In addition, they are constrained by Constitutional requirements that may not apply to commercial actors and that serves to further circumscribe their use of facial recognition technology. In the law enforcement context, some have questioned 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 certain 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 the Vermont example, the relevant question for legislators appeared to not have been whether notice and consent had been obtained, but rather, what the appropriate use of the technology is given law enforcement needs and constraints. Vermont police, presumably, did not want to alert potential child exploiters to the fact that they were being investigated and, as a

⁵¹ See *2021 Security Breach Legislation*, National Conference of State Legislatures, <https://www.ncsl.org/research/telecommunications-and-information-technology/2021-security-breach-legislation.aspx>.

result, notification to potential suspects and obtaining their consent would have frustrated the very law enforcement purpose the technology was being used for. However, the State of Vermont did indicate that the use of facial recognition technology by law enforcement merited other controls, and that any specific use be authorized by legislative action. 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), that necessitate an alternate framework for thinking about appropriate use of facial recognition technology.

There are also uses of facial recognition technology that involve people whose relationship with the government may complicate the ability of the government to obtain consent: criminal defendants, accused lawbreakers, people seeking government benefits, children, or people seeking access to public accommodations or locations for which there is a Constitutional right to access, for example. In the government's interaction with these categories of individuals, focusing on consent may not capture the risks and benefits of using facial recognition technology. In addition, freely given consent may not be possible as a result of the individual's lack of control vis-a-vis the government actor. 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, may not allow for meaningful consent, given that children are required to attend school and might not yet be of the age to provide legally binding consent. Similarly, 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. And, in contexts where people seek governmental benefits, consent may also be less meaningful. A person who is asked to consent to the use of facial recognition technology in order to access food benefits 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 prohibited in these circumstances, however, it does counsel that, given the individual's lack of control or meaningful choice and the nature of the relationship between the government and the individual, a notice and consent regime may not provide sufficient protections for the individual and society collectively.

For these applications—those that implicate Constitutional concerns or where individuals cannot freely or meaningfully consent, legislators and policymakers may find government use of facial recognition technology to be inappropriate, or that some other governing standards are necessary to protect individuals and society more broadly. Some of the potential governing standards in situations where neither an outright ban nor unfettered use is preferred are described below in Section VI.E, and may include 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. Notice and consent could be part of the considerations to be discussed or taken into account in designing the facial recognition technology use regime, but, by themselves, may be neither necessary nor sufficient to justify the use of the technology by a governmental entity alone.

- B. If a data subject's consent can be freely given, a notice and consent regime may be appropriate for government uses of facial recognition

Certain 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.⁵² 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 connection with a service that is optional from the perspective of the public. In other words, notice and consent may be appropriate when the public approaches the government service as consumers with an uncoerced choice about whether or not they wish to use the service, and the service will have negligible effects on our collective autonomy.⁵³

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 being considered should not be a monopoly, whether created by law or in fact, if the service can be 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. If the necessary 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 be just as unrealistic to apply a true consent regime under the circumstances as with a legally-imposed monopoly.

Second, 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. 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 "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

⁵² See *infra* Section VI.E.

⁵³ 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 Program⁵⁴ 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.⁵⁵ 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 facial recognition systems can be 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.

Fourth, 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.

C. Actual notice should be meaningful and transparent

To the extent that a notice and consent framework is appropriate, the notice should be meaningful and transparent.⁵⁶ As described above, facial recognition is a powerful tool that can have many benefits, but it can also pose a substantial risk to an individual's privacy and civil liberties. Individuals should therefore be given a meaningful opportunity to understand what is being asked of them, so that their consent—assuming that it is provided—can be informed and freely given.

There are three elements that the drafting team considered as necessary for notice to be meaningful and to provide the necessary transparency: timing, presentation, and content, each of which is addressed in turn below.

⁵⁴ https://www.hud.gov/topics/housing_choice_voucher_program_section_8;
<https://www.fns.usda.gov/snap/supplemental-nutrition-assistance-program>.

⁵⁵ Williams, et al., (2016), "Understanding Associations between Race, Socioeconomic Status, and Health: Patterns and Prospects," <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4817358/>.

⁵⁶ In defining what constitutes meaningful and transparent notice, the drafting team analyzed various existing statutes regulating biometrics and privacy more generally, and have cited language from those statutes throughout in this section and the next to provide legislators and policymakers with examples of how lawmakers have defined requirements around notice.

1. Timing of Notice

The notice must be given prior to the capture of a facial image to ensure that the individual understands why the data is being captured and can make an informed decision about the choice they are being asked to make.⁵⁷ Notice should also be provided sufficiently far in advance of collection to give the individual adequate time to consider the consequences of their decision. For example, if an individual is purchasing a ticket to a theme park online, but is not informed until they arrive at the park that facial recognition technology will be used at the park for security purposes, the timing of the notice does not give the individual the opportunity to make a meaningful choice about the use of the technology. On the flip side, providing notice too far in advance of obtaining consent could result in a scenario in which notice becomes less effective in disclosing to an individual the risks and benefits of the choice they are being asked to make.

In addition, the notice should be presented prior to the individual investing considerable time or effort in the enrollment process. Similarly, the notice should be provided prior to an individual paying any fees or entering payment information, or otherwise committing to proceed with any service agreement. These guardrails are designed so that individuals do not feel pressured to consent to the use of facial recognition technology because of the time or resources they may have already invested in the effort.

2. Presentation of Notice

Legislators and policymakers need to carefully consider the presentation of the notice to ensure that it is understandable to the individual being asked to consent to the use of facial recognition technology. When considering the presentation of the notice, legislators and policymakers should consider the following guidelines:

- The notice about the use of facial recognition technology should stand alone, and be independent from other notices, for example, apart from other legal or financial disclosures.⁵⁸
- The notice should be clearly labeled at the start of the document, with unambiguous language about its purpose, for example, “Notice of Facial Recognition Collection and Use.”
- The notice should be understandable to the average individual and not include legal jargon.⁵⁹

⁵⁷ For example, the CCPA requires that notice be provided at or before collection, Cal. Civ. Code § 1798.100(a)(1), as does the IL BPIA, 740 Ill. Comp. Stat. 14/15(b).

⁵⁸ The CPRA’s definition of consent specifies that “[a]cceptance of a general or broad terms of use or similar document that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent.” Cal. Civ. Code § 1798.140(h).

⁵⁹ For example, the regulations for the CCPA require that notice “use plain, straightforward language and avoid technical or legal jargon.” Cal. Code Regs. Tit. 11, Div. 1, Chap. 20 § 999.305 (a)(2)(a).

- The notice should be available in different languages, as appropriate.⁶⁰
- The notice should meet the Americans with Disabilities Act and Web Content Accessibility Guidelines to accommodate persons with disabilities.
- The notice should be easily viewable on any devices or mediums where it may be presented.⁶¹ For example, for devices, the text should reflow when presented on smartphones and tablets, so that users do not have to scroll right to follow the text; the font should not drop below 10 points on any device where it is displayed; and low contrast color combinations should be avoided. If the notice is being presented on a physical sign, it should not be obscured by objects, and it should be at eye level or higher, where an individual of average height will easily see it.
- The notice should be available to print or save from the point at which it is displayed on screen, or paper copies should be available for individuals to take with them.
- The notice should be succinct and be able to be read by a person of average reading within a reasonable amount of time, for example, 2 minutes or less.
- The notice should not use dark patterns, or use images or other language that is misleading. For example, using a picture of a camera to signify that facial recognition technology is being used would not suggest to most individuals that face templates were being created using the individual's image.

3. Content of Notice

The drafting team also considered the content of the notice, and what information needs to be provided to individuals about the information that is being collected, as well as how that information will be used and disclosed. At a minimum, legislatures and policymakers should consider requiring that the following disclosures are in the notice:

- The name of the legal entity collecting the biometric information, and the name of any other legal entities that will collect or have access to the biometric data being collected and used.
- A description of the information being collected, that makes clear facial images will be collected and that facial templates will be created from that data for facial recognition purposes.

⁶⁰ The regulations for the CCPA provide that notice should be available in the languages “in which the business in its ordinary course” provides information to consumers in California. Cal. Code Regs. Tit. 11, Div. 1, Chap. 20 § 999.305 (a)(2)(c).

⁶¹ One example of this in practice is the CCPA, which requires that notice at collection use a format that “draws the consumer’s attention to the notice and makes the notice more readable, including on smaller screens, if applicable.” Cal. Code Regs. Tit. 11, Div. 1, Chap. 20 § 999.305 (a)(2)(b). Washington’s House Bill 1493 also more generally provides that notice should be “given through a procedure reasonably designed to be readily available to affected individuals.” WASH. REV. CODE ANN. § 19.375.020.

- A description of how the data will be used, which should be granular and tailored only to present (as opposed to future) uses.⁶² This limitation to present uses would mean that any changes to permit new uses, would be material, and would therefore require re-consent under the consent principle, as described in more detail below.
- An explanation of which entities will have access to the biometric information and/or with whom it will be shared, and for what purposes.
- The retention period for the data, which must be finite and tailored to the specific uses for the biometric information.⁶³
- How individuals can opt out of any non-essential use or sharing of their biometric data.
- How individuals can revoke their consent or request to have their data deleted. This must be a simple process that requires no more than 1 minute to complete.
- A description of any risks to the individual of providing biometric information.
- How facial recognition data is protected, including deletion, or de-identification policies.
- Whether facial recognition may be shared with law enforcement, and under what circumstances that might occur.

D. Individual consent should be informed and express

To the extent that a notice and consent framework is appropriate, consent should be obtained prior to the use of facial recognition technology, and that consent should be informed and express.⁶⁴ Legislators and policymakers will want to take into account a number of considerations in determining what constitutes adequate consent under the circumstances.⁶⁵

1. Timing of Consent

Consent should be obtained from an individual prior to the collection of their facial image where the intended use of that facial image is to create a facial template and later use it for

⁶² The regulations for the CCPA requires that if a business intends to collect categories of personal information other than what was specified in the initial notice, a new notice must be provided at collection. Cal. Code Regs. Tit. 11, Div. 1, Chap. 20 § 999.305 (a)(5).

⁶³ IL BIPA, for example, requires informing the subject “in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used.” 740 Ill. Comp. Stat. 14/15(a)(2).

⁶⁴ 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.

⁶⁵ The IL BIPA requires “informed written consent.” The statute does not explicitly state what elements are required to make the consent “informed,” although it requires that the notice include certain disclosures, including the specific purpose and length of time for which the information is being collected, stored, and used. 740 Ill. Comp. Stat. 14/15(b).

verification or identification purposes.⁶⁶ Prior to collection should mean that an individual is given sufficient opportunity to consider the notice provided to them, be able to comprehend what it means, ask questions if applicable, and be able to make a meaningful decision whether to consent.⁶⁷

2. Consent should be informed

In order for consent to be valid, the entity using facial recognition technology must provide the individual sufficient information about the application and intended use so that the individual understands what information is being collected and why, as well as how that information will be used and shared. A critical part of ensuring that consent is informed is a notice that provides adequate disclosures about the use of facial recognition technology so that an individual can weigh the risks and benefits of consent, and understand the consequences of their decision. This is one of the reasons why notice should fully describe the implications of having one's data ingested into a facial recognition system. The principles of informed consent also require that an alternative to the use of facial recognition technology be provided, if a meaningful choice can be said to be made (unless, of course, the service itself that is being offered is facial recognition technology).

3. Consent should be express

Given the special risks posed by facial recognition technology, the drafting team recommends that legislators and policymakers require that consent be express rather than implied. This means that some affirmative step must be taken by the individual that clearly indicates their intent to consent to the capture and use of their image for facial recognition. Such express consent should be obtained not only for image capture, but for the templating, storage, and specific uses of the captured data. This is not to say that a separate consent needs to be obtained for each step in the process, but where a single consent is presented, it should encompass all such steps. There are many ways in which express consent may be obtained—by signing a hard copy form, clicking or checking a box on a form or electronic version of a form (or unchecking or unclicking a prefilled box on a form), sending a letter or an email—but the main distinction is that some affirmative action must be taken by the individual to manifest that they are making a meaningful choice (rather than a presumption that facial recognition technology is allowable).⁶⁸

On the most formal end of the spectrum, a valid, express consent may consist of a written, explicit, signature on 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 or an expiration date. That being said, effective express consent need not necessarily be written. Oral consent in person or via electronic means, or consent given as a result of taking some action after being told that such action will indicate express consent, may be sufficient in some circumstances. Legislators and policymakers should consider the type of use of facial recognition,

⁶⁶ For example, IL BPIA requires that a written release be obtained prior to the collection, capture, purchase, receipt through trade, or otherwise, of an individual's biometric identifier or biometric information. 740 Ill. Comp. Stat. 14/15(b).

⁶⁷ The CPRA defines consent as “any freely given, specific, informed and unambiguous indication of the consumer's wishes . . . , such as by a statement or by a clear affirmative action, signifying agreement to the processing of personal information relating to him or her for a narrowly defined particular purpose.” Cal. Civ. Code § 1798.140(h).

⁶⁸ The IL BPIA, for example, requires that the subject of the biometric information execute a written release. 740 Ill. Comp. Stat. 14/15(a)(3).

the duration of the use, the expiration of consent, the risk to the individual under the circumstances, and other factors in determining what type of express consent is most appropriate given the circumstances. At a minimum, express consent—whatever the mechanism—should be “opt-in” as opposed to “opt-out” (e.g., requiring a consumer to uncheck a pre-checked box to refuse consent). Legislators and policymakers should also understand that consent cannot be considered “express” if the underlying notice is deficient in light of the notice principles set forth in Section VI(C) above. Consent should also not generally be considered “express” if it is merely part of a “compound” consent (e.g., using the same check box for consent to facial recognition and consent for disclosure of medical information to a third party), buried amongst other consents, or contained in wrap-around or other electronic pop-up messaging applications.

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

Consent also should be freely given. In simple terms, this means that the individual consenting to the use of facial recognition technology should make a voluntary choice that is not coerced or obtained through deception. Legislators and policymakers should consider scenarios in which the nature of the relationship between the end user and the entity requesting consent to use facial recognition technology suggests that the choice to accept or decline the use of facial recognition technology is not truly voluntary. This may be the case in scenarios where the entity asking for consent is in a position of power over the individual, for example a public sector entity or an employer, or where the individual’s ability to choose a different provider may be limited, as with a healthcare provider. 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.⁶⁹ In some instances, this concern could be allayed by making clear to the individual that refusing consent will not result in adverse consequences, 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 they see on the store’s shelves and send targeted advertising. Although it could be argued that requiring consent to obtain a discount is coercive, such a proposal likely is more accurately characterized as an incentive. In either event, the drafting team generally would not consider such an incentive as creating 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

⁶⁹ See Sections VI.A & B of this commentary.

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 in order to obtain an otherwise unavailable 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 and housing, 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 (streets, parks, beaches).

Another scenario in which consent may not be considered to be freely given is when such consent is obtained through the use of dark patterns, or other user interfaces or interactions that are manipulative or deceptive by design.⁷⁰ When a user interface/user experience is designed in a manner that is likely to confuse an individual about the choices they are making, or how to indicate the choices they wish to make (for example, the use of double negatives, opt-out slide bars with unclear or contradictory explanations, or default settings that are inconsistent with a reasonable individual’s expectations), there is no reason to conclude that “consent” provided under those circumstances corresponds to an actual volitional choice.

5. Secondary use and transfer should require additional consent

Secondary uses of facial recognition data—uses that are materially different than what was presented at the time of collection and initial consent—will require subsequent, affirmative consent. In addition, the parameters for consent to 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. To avoid situations where consent to future use is treated as an unconditional license for all secondary uses, 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 would not otherwise be able to identify the individual.⁷¹

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 should be required to allow individuals the choice to opt into the collection and use of data by the collecting entity for its primary purpose, but decline to consent to secondary use(s) or transfer of data to a third party. Such layered consent requirements should not necessarily apply to third-party vendors

⁷⁰ Under the CPRA, consent cannot be obtained through dark patterns. Cal. Civ. Code § 1798.140(h).

⁷¹ Future of Privacy Forum, *supra* note 61.

contracted by the entity using the facial recognition technology to carry out the uses in the entity's original disclosure.

6. Consent should be freely revocable

Subject to reasonable technological limitations, individuals should have the right to revoke their consent. In many circumstances where an individual wishes to revoke their consent (for example, the individual no longer works for a company that uses 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.⁷² However, the "right to be forgotten" as embodied in the General Data Protection Regulation⁷³ and statutes such as California's Consumer Privacy Act and Privacy Rights Act⁷⁴ 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 develop (or "train") a facial recognition system. Many commercial systems are used in situations in which data subjects are required to consent to use of the system (in connection with taking an online college entrance or professional certification examination, for example); such scenarios often also require the data subject's nominal consent to the use of their data in the improvement of the facial recognition system itself.⁷⁵

For some time, 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. The matter is complicated by the fact that the exact details of how a particular trained facial recognition AI algorithm (artificial neural networks in particular) often are not entirely understood by the developers of the systems themselves. This lack

⁷² We note that individuals requesting deletion of their data from a facial recognition system gallery database may, ironically perhaps, be required to provide a photograph of themselves for purposes of identifying that user's data in the system, or as part of the authentication process.

⁷³ See generally GDPR Article 17, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e2606-1-1>.

⁷⁴ 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.

⁷⁵ 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. 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).

of transparency results from the system itself independently making many of the determinations about how to evaluate the data to conduct the facial recognition task.

Although no image data of any particular individual exists in a facial recognition algorithm *per se* (that is, no individual's image or template data could be retrieved directly from the system model itself), in theory at least, 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.⁷⁶ This is despite the fact that neither the GDPR nor the various EU Member State 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. Nor have they addressed the related question of whether a system owner may avoid a deletion request as to machine learning model training impact if the owner can establish the impossibility or impracticability of deleting the training impact of an individual's data.⁷⁷ 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 GDPR rights (such as the data portability right⁷⁸), the right of deletion under GDPR Article 17 contains neither an 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.⁷⁹ That being said, legislators and 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 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.⁸⁰ Countermeasures and protections, including those based on differential privacy and other

⁷⁶ 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.

⁷⁷ Villaronga, et al., (2018) “Humans Forget, Machines Remember,”

https://scholarship.law.bu.edu/faculty_scholarship/817/.

⁷⁸ *See* Article 14(5)(b), <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e2355-1-1>.

⁷⁹ Article 17(2), <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e2606-1-1>.

⁸⁰ Fredrikson, et al., (2015) “Model Inversion Attacks that Exploit Confidence Information

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.⁸¹

Given the lack of consensus as to the scope of the right to deletion in the context of AI systems, barring the implementation of a strong anonymity solution with a firm basis in data science, as a practical matter, the only way to be sure that a single individual's data is securely removed from a recognition model may be to retrain the entire algorithm from scratch, *i.e.*, as it existed prior to any training.⁸² Given the massive amount of technological 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 an individual. Legislators and policymakers will therefore need to consider whether there are some circumstances in which individuals should not have the right 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/or where the personal data cannot reasonably be deleted without frustrating the purpose for which it was originally used.

- E. Entities must take measures to ensure accountable and transparent use of facial recognition technology, especially where providing notice and obtaining consent are not feasible

Where a notice and consent framework is not appropriate, legislators and policymakers should implement measures to ensure that the entities deploying the technology are held to transparency and accountability standards. Although the transparency and accountability measures outlined below are intended to provide additional protections where notice and consent are not feasible (which is primarily in the law enforcement and national security context, but also for certain other government uses as described earlier in this Commentary), entities providing notice and obtaining consent to uses of facial recognition technology also would benefit from consideration of these issues. The considerations outlined below could be implemented in full, but not all measures may be necessary to ensure adequate accountability given the particular circumstances at play. The goal is less to prescribe a specific approach, but rather to model a cohesive strategy that could be used by legislators and policymakers to ensure that the risks identified in Section V of this commentary are adequately mitigated.

One way to think about transparency and accountability are as community-wide mechanisms to achieve policy goals similar to those intended by notice and consent, or even to actually ensure appropriate notice and consent in their broadest, societal, sense. Transparency is necessary to

and Basic Countermeasures,” <https://www.cs.cmu.edu/~mfredrik/papers/fjr2015ccs.pdf>.

⁸¹ 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).

⁸² 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.

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 cannot be relied on to protect individual rights. Both transparency and accountability measures, especially those that create an opportunity for stakeholder review of a prospective plan of use and penalties for abuse, may be regarded as constituting a form of implied or constructive consent by the affected community as a whole. In that way, the citizenry is provided notice of the intended use of facial recognition technology and, through the legislative process, has an opportunity to reject the plan or, by inaction, to assent. This paradigm could be supported by a broader standing legal mandate that stakeholder review of a detailed implementation and use plan is a prerequisite to any facial recognition implementation or deployment by a governmental body or government contractor; and laws prohibiting the misuse or abuse of a government owned, operated, or contracted facial recognition system that include effective sanctions for violation.

Such a legal foundation would ensure that legislatures and government executives have a meaningful opportunity to evaluate and respond to uses of facial recognition technology, and to invoke appropriate legislative and/or administrative processes. The plans for prospective use may be general enough to protect operational success and law enforcement officer safety, for example (including in limited instances by restricting review of portions of the plan to select legislative or executive committees as specifically necessary), 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 and balance, for example:

- The permissible persistence and pervasiveness of surveillance.
- Whether the proposed use unjustifiably and broadly surveils without notice those who are not the subject of reasonable criminal suspicion.
- Whether the use is generally consistent with Fourth Amendment and other criminal procedure 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.⁸³

⁸³ This assessment should be made based on the personnel 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

- Whether the data against which any matching is performed is compiled from permissible sources.
- Whether the image and template data of the system will be properly protected from misappropriation or other improper use, or loss of integrity.
- 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 clearly defined and will be applied consistently according to specified neutral principles.
- Whether operators of the system are trained in proper usage of the system.
- Whether practicable alternatives to the use of facial recognition technology are cost-prohibitive or impracticable.
- The concrete benefits to the efficiency of the mission of the governmental entity.
- The administrative, physical, and technical controls that will be implemented and maintained to prevent misuse/abuse or compromise of the system, including intra-entity sanctions that will be imposed for violations.
- The risk of unapproved secondary uses that may be made of any information generated or collected through the system or its use.

One mechanism to ensure accountability and the creation of transparent and detailed plans would be for legislators and policymakers to adopt standards for such plans, which could draw from the elements outlined above. The particular standards adopted by policymakers and legislators ultimately would 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 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

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.

community is unwilling to tolerate. Such an approach would ideally 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 to address in 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 suitable for one use, (such as developing a photo array), and not fit for another (such as 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 at issue 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 circumstances where the technology would be useful, but were not anticipated by the entity in its prospective use plan. The aim is to ensure that these unanticipated 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 certain uses may be permissible even though they were not previously disclosed. These could include, 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 thus 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 facial recognition technology. For example,

one approach could be civil sanctions against the law enforcement officers who authorized or directed deployment of the technology, with the potential for criminal sanctions in the case of gross departures from the requirements that were demonstrably made recklessly or in bad faith.

Finally, the mechanisms for transparency and accountability described above simply propose a framework by which entities can provide constructive notice to the community that 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 evidentiary rules may 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 used in court to identify 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.

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

Appendix A:⁸⁴

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, which includes biometric information in its definition of “protected personal information.” 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.

- **Arkansas House Bill 1943**

- Arkansas passed House Bill 1943 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.

- **California Body Camera Accountability Act - Assembly Bill 1215**

- AB-1215 went into effect in January 2020 and imposes a 3-year moratorium on use of FRT in police body cameras. The bill 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)**

- BIPA was 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) requires a company to provide specific notice and obtain consent from the particular person whose biometric information is collected. 740 ILL. COMP. STAT. 14/15(b). BIPA also bans the sale or trade of personal biometric information for profit. 740 ILL. COMP. STAT. 14/15(c). BIPA provides for a private right of action for anyone “aggrieved by a violation” of the statute. 740 ILL. COMP. STAT. 14/20.

- **Louisiana Database Security Breach Notification Law**

- The Louisiana Database Security Breach Notification Law was 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

⁸⁴ Unless otherwise noted, “biometric” information under the laws listed herein includes facial recognition technology.

“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 limited to actual damages arising from failure to timely notify.

- **Maine “Act to Increase Privacy and Security by Regulating the Use of Facial Surveillance Systems by Departments, Public Employees and Public Officials”**
 - Under **LD-1585**, which went into effect on October 1, 2021 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. 25 M.S.R.A § 6001 (2)(A). Law enforcement may use the technology for investigating certain serious crimes, but state law enforcement agencies are barred from implementing their own FRT systems. M.S.R.A § 6001 (2)(B). They may request FRT searches from the FBI and the state Bureau of Motor vehicles in certain cases. M.S.R.A § 6001 (2)(C). 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.” M.S.R.A § 6001 (2)(A). 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. M.S.R.A § 6001 (2)(B). 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. M.S.R.A § 6001 (2)(C).
- **New Hampshire**
 - Applicable to “any law enforcement agency that elects to equip its law enforcement officers with body-worn cameras [(BWC)]” New Hampshire has banned police numerous processing activities of footage from BWC footage, “including but not limited to facial recognition technology.” NW REV STAT § 105-D:2 (2017). There is an exception for “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.
- **Oregon Laws**

- Although it does not specify facial recognition technology, the **Consumer Information Protection Act** amended Oregon’s breach of notification law to include in 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).
- **ORS 133.741** effectively bans the use of FRT in police body cameras by requiring 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**
 - Texas requires companies who collect biometric data for commercial purposes to inform the individual and receive the individual’s consent. TEX. BUS. & COM. CODE ANN. § 503.001. Consent must also be obtained for a possessor of biometric information to sell, lease, or disclose that information and must store, transmit, and protect using “reasonable care.” TEX. BUS. & COM. CODE ANN. § 503.001. 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.
- **Vermont S. 124**
 - S.124 prohibits 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. The law was modified in May 2021 in H.195 to carve out use of FRT in criminal investigations of sexual exploitation of children.
- **Virginia HB 2031**
 - 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**
 - House Bill 1493, requires protections for consumers’ biometric information. , imposing a consent requirement for the collection and commercial use of biometric

information, and setting a reasonable care standard for possessors to guard against unauthorized access and limited retention of the information. WASH. REV. CODE ANN. § 19.375.020 Washington later amended its breach notification law to include biometric information as “personal information.” 2019 WASH. H.B.1071.

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.
- **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, San Francisco prohibited government agencies and law enforcement from using FRT, 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.

- **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 provides that city officials and entities cannot “obtain, retain, possess, access, sell, or use any prohibited surveillance technology or information derived from a prohibited surveillance technology.” An exception allows the use evidence obtained through FRT 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.** The 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.

- **Massachusetts**

- **City of Boston.** Ordinance #0683, 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. The ordinance provides a private right of action, including 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.
- **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. The law provides a private right of action, including 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 ordinances enacted in September 2020, prohibit not just government FRT use but also many applications of facial recognition by private entities. The first ordinance took immediate effect and bans the use and acquisition of face recognition technologies by City bureaus and applies to all City of Portland bureaus and offices. The second ordinance went into effect January 1, 2021, and bans private entities from using facial recognition technology in places of public accommodation and included all private entities in Portland.

- **Pennsylvania**

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

- **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. The law includes a number of exemptions. FRT can be used to identify and/or locate individuals who are victims of human trafficking or missing children. It 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 it 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.

© 2022 The Sedona Conference

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

Appendix C

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 the drafting team 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.⁸⁵ 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.”⁸⁶ 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.”⁸⁷ 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.”⁸⁸
- The FTC issued recommended best practices for facial recognition technology in its *Best Practices for Common Uses of Facial Recognition Technologies* staff report.⁸⁹ 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.⁹⁰ 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

⁸⁵ 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.

⁸⁶ *Id.* at 8.

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ 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.

⁹⁰ *Id.* at ii.

that data will be used.⁹¹ 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.⁹² The FTC report also envisions affirmative express consent being necessary in two scenarios.⁹³ 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 Information Practice Principles.⁹⁴ 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 consent, 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.”⁹⁵ The principles explain that these policies or disclosures 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.⁹⁶ Although these principles do envision covered entities providing notice to consumers, they do not provide consumers

⁹¹ *Id.*

⁹² *Id.*

⁹³ 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.

⁹⁴ 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. See 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.

⁹⁵ NTIA *Privacy Best Practice Recommendations for Commercial Facial Recognition Use*, *supra* note 95 at 2.

⁹⁶ *Id.* at 2.

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.⁹⁷ 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*.⁹⁸ 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 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.”⁹⁹ 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.¹⁰⁰ 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.¹⁰¹ The principles also envision circumstances where notice is required, but opt-out consent is sufficient. These included templates created within online 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.¹⁰² 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

⁹⁷ *Id.* at 2.

⁹⁸ 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.

⁹⁹ *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 3 n.7.

¹⁰⁰ *Id.* at 3.

¹⁰¹ *Id.* at 4.

¹⁰² *Id.* at 4.

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

data.¹⁰³ 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.¹⁰⁴

¹⁰³ *Id.* at 6.

¹⁰⁴ *Id.* at 6.