

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



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

## TABLE OF CONTENTS

	Page
I. INTRODUCTION .....	1
II. HOW FACIAL RECOGNITION TECHNOLOGY WORKS .....	2
III. USES OF FACIAL RECOGNITION TECHNOLOGY .....	5
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. CRITICISM OF NOTICE AND CONSENT AS A LEGAL FRAMEWORK .....	15
VII. PRINCIPLES .....	18
A. Principle 1: Legislators and policymakers should recognize the limitations of notice and consent for facial recognition technology .....	18
B. Principle 2: Notice and consent can be compatible with lower risk uses of facial recognition technology .....	19
C. Principle 3: Notice must be transparent, consent must be informed .....	20
1. Notice .....	21
2. Consent.....	22
D. Principle 4: Substantive limitations offer important protections, even for lower risk uses.....	26
1. Purpose Limitation .....	26
2. Reasonable Data Security.....	27
E. Principle 5: Notice and consent offer insufficient protection for higher risk uses ..	29

## I. INTRODUCTION

The relatively 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.<sup>1</sup> 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.

This Commentary addresses whether, under what circumstances, and how laws requiring notice to and consent of an individual should be used in connection with the collection, creation, use, and disclosure by the private and public sectors of that individual's biometric facial recognition data.<sup>2</sup> The Commentary proposes a set of legal principles to guide legislators and policymakers in deciding when notice and consent can be relied upon, what that notice and consent should look like, and whether certain substantive limitations should be implemented along with or in lieu of notice and consent to guard against certain risks attendant to the technology.<sup>3</sup>

Section II of the Commentary provides a basic overview of how facial recognition technology works,<sup>4</sup> while Section III provides examples of common uses of the technology. Section IV describes how the technology is currently regulated, with a particular focus on the

---

<sup>1</sup> See, e.g., Privacy Act of 1974, Public Law No. 93-579, as amended, codified at 5 U.S.C. § 552a; 15 U.S.C. 45 (Section 5 of the Federal Trade Commission ("FTC") Act).

<sup>2</sup> 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). *Id.*

<sup>3</sup> 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.

<sup>4</sup> 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 Biometric Privacy Primer (hereinafter Biometric Primer) provides a more comprehensive overview of biometric technologies generally, including facial recognition technology.

United States<sup>5</sup>, 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. Section VI explores some of the criticism around notice and consent and, in particular, its application to facial recognition technology. Finally, Section VII encompasses a series of guidelines that provide legislators and policymakers with direction on when, and what sort of, a notice and consent framework may be appropriate for facial recognition applications. For certain lower risk facial recognition applications, it discusses what should constitute adequate notice and consent, as well as minimum substantive limitations that should be put in place to ensure adequate protections. This section also posits that notice and consent might well be found by legislators and policy makers to be incompatible with or insufficient to fully address certain higher risk uses of facial recognition technology, primarily identification uses, and offers recommendations for legislators and policymakers that make such a finding on measures to ensure accountability and transparency for such uses.

Given the potential breadth of the topic, 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),<sup>6</sup> or facial detection (determining whether a human face is 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 authors of this commentary believe the unique characteristics of facial recognition technology necessitate heightened protections. Finally, this commentary also does not address considerations around 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.<sup>7</sup> 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.<sup>8</sup> 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, as explained below) 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

---

<sup>5</sup> Although many jurisdictions are actively debating how to regulate facial recognition technology, we have largely focused on the current U.S. approach for purposes of Section IV given that jurisdiction’s historical tendency to rely on notice and consent as a basis for regulating digital technologies.

<sup>6</sup> 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).

<sup>7</sup> *See, generally*, Biometric Primer (2022).

<sup>8</sup> 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.

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:<sup>9</sup>

***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).<sup>10</sup>

***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.<sup>11</sup> 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. The system also eliminates “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 image<sup>12</sup> already stored in or accessible by the facial recognition system.

---

<sup>9</sup> 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.

<sup>10</sup> 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).

<sup>11</sup> 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.

<sup>12</sup> In some facial recognition systems, the system may merely store template data derived from images, 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.

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:<sup>13</sup>

- 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.<sup>14</sup> Here the goal is aimed at authenticating an individual to verify that a person is who she or he claims to be, and the process relies on the comparison of two templates.<sup>15</sup>
- 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.<sup>16</sup> Here the system must carry out a test on each face captured to generate a biometric template and check whether it matches a person known to the system.<sup>17</sup> Identification can be used to find a person among a group of individuals, in a specific area, or an image in a database.<sup>18</sup>

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

---

<sup>13</sup> Various algorithms have been implemented to perform this comparison, from more conventional, deliberately designed algorithms that 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 similar template data for different images of the same person by using data points developed by the neural network itself—it may not be entirely clear to the developers of the system exactly how these data points are used to create a template, or even what data points the system primarily considers. Empirically, however, these systems may prove to be more accurate than traditionally designed algorithms.

<sup>14</sup> The most common example of such 1:1 verification will be when an individual presents their face to unlock a mobile phone or other computing device. As another example of 1:1 verification involving a large gallery, the user may be a traveler or immigration official presenting the query image of the traveler just taken at a national port of entry kiosk, to be compared against the single gallery image (also called a "reference image" in the verification context) of the traveler's official ID photo stored by the immigration agency.

<sup>15</sup> European Data Protection Board, *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement Version 1.0*, at 7 (Adopted May 12, 2022) (hereinafter *EDPB Guidelines*).

<sup>16</sup> 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.

<sup>17</sup> *EDPB Guidelines*, at 7.

<sup>18</sup> *Id.*



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 person<sup>19</sup>), but it turns out that the person in the query image was not in fact the same person returned by the system from the gallery database, this erroneous hit is called a “false positive.”

In the case of identification (one-to-many matching), if the system finds one or more potentially “matching” images from the image gallery, typically these images will be returned to the user as output, together with any information corresponding to the gallery images such as the names and other identifying information of the people depicted in the returned gallery images. Depending on the design and use of the system, the output to the user will usually also include the system’s confidence about the match (e.g., how “good” the match was in mathematical terms), and the query image, particularly if the person in the query image is not present at the use site. As with the verification application, a facial recognition system can make errors in its determination. In particular, the error rate (both of false positives and false negatives) disproportionately affects people of color and women and constitutes a unique risk in the widespread adoption of the technology.<sup>20</sup>

### III. USES OF FACIAL RECOGNITION TECHNOLOGY

The use of facial recognition technology for a wide variety of purposes has grown quickly 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.<sup>21</sup>

---

<sup>19</sup> 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.

<sup>20</sup> See *infra* Section V.A.

<sup>21</sup> See Biometric Primer, Section III.A., for a broader discussion of the uses and benefits of biometric technology.



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.<sup>22</sup>
- ***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.<sup>23</sup> Facial recognition technology may also be used to verify the identity of travelers at airports, and to authenticate the identity of employees entering a secure location in an office or factory.
- ***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.
- ***“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

---

<sup>22</sup> 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).

<sup>23</sup> A familiar example is the use of facial recognition technology to unlock a smartphone or to log in to a camera-enabled computer.

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 in the United States. Instead, for federal applications, the Privacy Act generally regulates its use, and the Federal Trade Commission also regulates its use under Section 5 of the FTC Act. 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 regulations that could apply to public sector<sup>24</sup> or private sector uses of facial recognition technology depending on the particular circumstances:<sup>25</sup>

- **Privacy Act**
- **Section 5 of the Federal Trade Commission Act**
- **State data breach notice laws**
- **State biometric privacy laws**
- **State and local facial recognition restrictions or regulations**

At the federal level, 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. The FTC also regulates the use of facial recognition technology under its general Section 5 authority, both by bringing enforcement actions and through guidance. For example, in January 2021, the FTC settled with a photo app developer that used facial recognition technology to group users' uploaded images.<sup>26</sup> As part of the consent order, the developer agreed to provide notice separate from a privacy policy or terms of use detailing "all purposes for which [the developer] will use, and to the extent applicable, share" biometric information and obtain users' "affirmative express consent" prior to using facial recognition technology on users' images.<sup>27</sup> In 2012, the FTC released a staff report that suggested best practices for the commercial use of facial recognition technology,

---

<sup>24</sup> Although there are few federal laws that govern the use of facial recognition technology by the federal government, the United States Government does collect and use 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 U.S. For example, the U.S. Department of Homeland Security ("DHS") provides biometric identification services to protect the nation through its Office of Biometric Identity Management, which generally follows the Fair Information Practice Principles (FIPPs) as the foundation for privacy policy at DHS, and which routinely engages in privacy impact assessments for its uses of biometric information.

<sup>25</sup> An overview of some of the laws and ordinances identified and surveyed by the drafting team can be found at Appendix A.

<sup>26</sup> FTC Press Release, *California Company Settles FTC Allegations It Deceived Consumers about use of Facial Recognition in Photo Storage App* (Jan 11, 2021).

<sup>27</sup> *In the Matter of Everalbum, Inc.*, FTC File No. 1923172, Agreement Containing Consent Order, at 4.

including that companies provide notice and choice, implement “privacy by design” and have reasonable data security protections in place.<sup>28</sup>

The drafting team also considered state and municipal approaches to regulating the technology. 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”)<sup>29</sup> 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. It also imposes civil penalties in the case of a breach but not a private right of action. Arizona, Louisiana, New York, Oregon, and Washington have data breach notice laws with similar approaches.<sup>30</sup>

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.<sup>31</sup> BIPA also requires a company to provide specific notice and obtain consent from the particular person whose biometric data is collected.<sup>32</sup> Further, it bans the sale or trade of personal biometric data for profit.<sup>33</sup> BIPA provides for a private right of action for anyone “aggrieved by a violation” of the statute.<sup>34</sup> The Texas Business and Commerce Code § 503.001 bans the use of biometric data for commercial purposes without prior notice and consent, and provides for enforcement through a civil penalty of up to

---

<sup>28</sup> FTC Staff Report, *Facing Facts: Best Practices for Common Use of Facial Recognition Technologies* (Oct. 2012).

<sup>29</sup> 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.

<sup>30</sup> The Louisiana and Washington laws include a private right of action for a failure to timely notify in the event of a data breach.

<sup>31</sup> 740 Ill. Comp. Stat. 14/15(a).

<sup>32</sup> *Id.* at 14/15(b).

<sup>33</sup> *Id.* at 14/15(c).

<sup>34</sup> *Id.* at 14/20.

\$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. The law 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, however, 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. 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.<sup>35</sup> New Hampshire and Oregon ban police from using facial recognition technology in body cameras used by police. Although Virginia had prohibited local law enforcement and campus police from purchasing or deploying facial recognition technology unless expressly authorized by state statute, in 2022, it changed course and now authorizes local law enforcement and campus police to use facial recognition technology for certain “authorized uses,” including to help identify an individual where there is a reasonable suspicion the individual has committed a crime, to help identify a crime victim or missing person, and to help identify a person who is reasonably believed to be a danger to himself or others.<sup>36</sup>

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

---

<sup>35</sup> The California moratorium went into effect January 2020.

<sup>36</sup> SB 741, VA Legislature 2022 Session, Facial Recognition Technology; Authorized Uses.

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 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.”<sup>37</sup> The Portland, Oregon, ban contains a private right of action, with statutory damages of \$1,000 per day.<sup>38</sup> 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.”<sup>39</sup>

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. One bill introduced in 2022 would place limitations and prohibitions around the use of the technology by law enforcement. Others introduced in recent years would 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 four 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

---

<sup>37</sup> Portland, OR., City Code Ch. 34.10 (2020).

<sup>38</sup> *Id.*

<sup>39</sup> *Id.*



reasoning and considerations behind the guidance. A description of some of the principles that the drafting team considered can be found in Appendix C.

## 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 and Data Security 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.<sup>40</sup> 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.<sup>41</sup> 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. Data security concerns include that the algorithm and protected template are either exfiltrated and/or that the algorithm is modified, or that an unauthorized template is injected into the system.
- **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

---

<sup>40</sup> See FTC Staff Report, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, at 7-8 (2012) (citing concerns of commenters).

<sup>41</sup> 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).

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 this technology ever violates a person’s “reasonable expectation of privacy” under the Fourth Amendment.<sup>42</sup>
- **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.<sup>43</sup>
- **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.”<sup>44</sup> 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.<sup>45</sup> 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.”<sup>46</sup> Deficiencies in the technology have led to real world examples where facial recognition systems have

---

<sup>42</sup> *Katz v. U.S.*, 389 U.S. 347, 361 (1967).

<sup>43</sup> 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).

<sup>44</sup> See *Simmons v. United States*, 390 U.S. 377, 384 (1968).

<sup>45</sup> See Larry Hardesty, *Study Finds Gender and Skin-Type Bias in Commercial Artificial Intelligence Systems*, MIT News Office, (Feb. 11, 2018).

<sup>46</sup> Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use*, WASHINGTON POST (Dec. 19, 2019).



misidentified people of color, leading to their wrongful detention or arrest.<sup>47</sup> Among other issues, many commonly used datasets contain imbalanced demographic distributions that result in biased discrimination when used to train facial recognition models. A database of images used to train the software may be so small and so racially skewed that the resulting algorithm is less reliable when matching people of color than it is in matching those of Anglo-European descent.<sup>48</sup> 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.<sup>49</sup> 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.

- **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 adequately protect biometric data.<sup>50</sup> 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.
- **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

<sup>47</sup> 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).

<sup>48</sup> Harwell, *supra* note 34.

<sup>49</sup> 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.

<sup>50</sup> See *2021 Security Breach Legislation*, National Conference of State Legislatures, <https://www.ncsl.org/research/telecommunications-and-information-technology/2021-security-breach-legislation.aspx>.

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.<sup>51</sup>

- **Litigation Risk.** In recent years, there has been a sharp rise in class action litigation related to the misuse of facial recognition technology, largely under Illinois's Biometric Information Privacy Act. One of the most notable lawsuits brought under Illinois's BIPA was a class-action lawsuit brought by Illinois consumers claiming that Facebook collected and stored the biometric data of millions of consumers without their consent as part of Facebook's "tag suggestions" feature.<sup>52</sup> Facebook eventually settled this case for a landmark \$650 million.<sup>53</sup> 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.<sup>54</sup> 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.<sup>55</sup> 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.<sup>56</sup> In less controlled settings, such as when there is bad lighting or where faces may be obstructed, the likelihood of misidentification increases.<sup>57</sup> 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.<sup>58</sup>
- **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

---

<sup>51</sup> 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).

<sup>52</sup> *In re Facebook*, 2018 U.S. Dist. LEXIS 81044, at \*3.

<sup>53</sup> See Jennifer Bryant, *Facebook's \$650M BIPA settlement 'a make-or-break moment'*, IAPP (Mar. 5, 2021), <https://iapp.org/news/a/facebooks-650m-bipa-settlement-a-make-or-break-moment/>.

<sup>54</sup> 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->.

<sup>55</sup> *Id.*

<sup>56</sup> 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>.

<sup>57</sup> *Id.*

<sup>58</sup> See, e.g., K. Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, NY TIMES (Dec. 29, 2020).

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.

## VI. CRITICISM OF NOTICE AND CONSENT AS A LEGAL FRAMEWORK

Notice and consent has been the dominant legal framework through which people engage with digital technologies in the U.S. This notice and consent framework has particular appeal given that society's emphasis on individual liberty and autonomy. Where people are given the option of agreeing to or declining to permit a certain use of their personal data, they may feel some measure of "control" and decision-making authority over how their information is used.<sup>59</sup>

The reliance on notice and choice to ensure adequate personal information privacy protection for digital technologies can be traced back at least to the United States Department of Health, Education, and Welfare's seminal 1973 report in which it outlined a set of FIPPs.<sup>60</sup> Over the ensuing years, variations on these principles have been articulated by a number of governmental and inter-governmental agencies, including by the Federal Trade Commission.<sup>61</sup> The FTC distilled the FIPPs, which it described as "widely-accepted as essential to ensuring that the collection, use, and dissemination of personal information are conducted fairly and in a manner consistent with consumer privacy interests" to five principles.<sup>62</sup> The first of the principles, notice/awareness, was described as "the most fundamental principle" and as a necessary predicate to the second principle, "choice/consent," which "means giving consumers options as to how any personal information collected from them may be used," either through an opt-in or opt-out regime.<sup>63</sup>

This notice and consent framework is prevalent across the U.S. privacy landscape. Core privacy laws, like the Gramm-Leach Bliley Act Privacy Rule, revolve around notice and consent. That law requires financial institutions to explain their information sharing practices to customers and provide those customers a limited right to control whether their information is shared with certain third parties.<sup>64</sup> The state biometric privacy laws also are grounded in notice and consent. For example, the Texas Capture or Use of Biometric Identifier (CUBI) Law prohibits the capture of a biometric identifier unless the individual has been informed prior to capture, and the individual consents to the capture.<sup>65</sup> Even newer state comprehensive privacy laws, such as the CCPA/CPRA in California, have detailed notice requirements, as well as opt-out / opt-in requirements for certain data uses.

---

<sup>59</sup> See Neil Richards and Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 Washington University Law Review 1461, 1461 (2019).

<sup>60</sup> See Federal Trade Commission, [Privacy Online: A Report to Congress](#), f. 27 (June 1998) (hereinafter *1998 FTC Report*).

<sup>61</sup> *Id.*

<sup>62</sup> *Id.* at 7. The five principles as articulated by the FTC in its *1998 FTC Report* were: (1) Notice/Awareness, (2) Choice/Consent, (3) Access/Participation, (4) Integrity/Security, and (5) Enforcement/Redress. *Id.* at 7.

<sup>63</sup> *Id.* at 7-9.

<sup>64</sup> See, e.g., 12 CFR Part 40.

<sup>65</sup> Capture or Use of Biometric Identifier Law, Texas Business and Commerce Code, Title 11, Ch. 503, Section 503.001(b).

Despite the prevalence of notice and consent in the U.S. as the approach to regulating digital technologies, observers increasingly pay attention to its shortcomings. In particular, questions of whether such a framework offers adequate protection where technology is pervasive and nascent enough that harms may still be difficult to foresee or hard to quantify are openly being debated. Data use terms may be so detailed and nuanced as to be impossible to understand for the average person. People may feel they have little choice but to accept the terms that entities offer given how essential networked devices and online services are to navigating daily life. The concern here is that mere reliance on notice and consent as a basis for processing personal data given present realities — without something more—does not provide people nearly the level of information and power that is associated with informed and freely given consent. Lina Kahn, Chair of the FTC, has emphasized this point, criticizing the notice and consent paradigm as outdated and insufficient:

Many have noted the ways that this framework seems to fall short, given both the overwhelming nature of privacy policies—and the fact that they may very well be beside the point. When faced with technologies that are increasingly critical for navigating modern life, users often lack a real set of alternatives and cannot reasonably forego using these tools.<sup>66</sup>

The alternative, as espoused by Chair Kahn and others, is to look beyond notice and consent—or procedural protections—to more substantive limits on the use of certain technologies. Whereas procedural protections address personal data processing by governing the methods by which people and data collectors interact, substantive protections place limitations on what information can be collected in the first place and how it can be used, regardless of whether or not an individual consents. Many non-U.S. jurisdictions have moved towards data protection laws that are principle based, restrict certain practices, and/or require increased accountability for the entity processing personal data, which are all examples of substantive limitations. For example, the GDPR lays out six principles that apply to personal data processing, including that it be processed lawfully, fairly, and in a transparent manner, that the data be accurate, and that only the least amount of data necessary to achieve a particular purpose be processed.<sup>67</sup> In addition, the GDPR imposes data security and role-based obligations, and provides data subjects with certain rights in relation to their personal data. The GDPR also deemphasizes the importance of consent, by limiting the processing of personal data to six lawful bases.<sup>68</sup> While consent is one of those lawful bases, many entities have moved away from a reliance on consent to justify processing given the high-standards imposed by the GDPR on what is necessary in order for consent to be valid and the fact that it can be revoked at any time.<sup>69</sup>

In addition to more generalized concerns about the adequacy of notice and consent, there has also been some scholarship regarding whether notice and consent can ever be appropriate for facial recognition technology specifically. Indeed, the reaction of many jurisdictions to ban the technology outright is an implicit rejection of the notice and consent model and suggests that some other way of regulating the technology is needed in order to adequately protect individuals and our larger societal values. In their paper *The Inconsistency of Facial Surveillance*, Evan Selinger and Woodrow Hartzog argue that consent can never be a valid legal basis for facial recognition

---

<sup>66</sup> Federal Trade Commission, Remarks of Chair Lina M. Kahn, As Prepared for Delivery IAPP Global Privacy Summit 2022, Washington DC (April 11,

<sup>67</sup> GDPR, Article 5.

<sup>68</sup> *Id.* at Article 6.

<sup>69</sup> *See* GDPR, Article 7, Conditions for Consent.

surveillance.<sup>70</sup> According to the authors, in order for consent to facial surveillance to be knowing and voluntary, at least three pre-conditions must exist: (1) such a request should be infrequent, (2) the harms to be weighed must be tangible, and (3) there should be incentives to take each request for consent seriously.<sup>71</sup> In their view, requests for consent to facial recognition technology are already too frequent and confusing such that people have become overwhelmed and desensitized.<sup>72</sup> They also argue that there is a virtual panoply of harms that can result from the use of facial recognition technology, including a loss of obscurity, chilling of speech, and increased discrimination against marginalized groups, among others.<sup>73</sup> These harms are less tangible due to the fact that—at least for now—they seem far off, are framed in abstract notions of a loss of privacy or autonomy, and the public “is routinely given seemingly good reasons to believe that the social benefits caused by consenting to surveillance would outstrip any social harms.”<sup>74</sup> Finally, they argue that people do not take each request for consent seriously, as each request only chips away at people’s rights and freedom, such that no single decision represents a significant threat.<sup>75</sup> In Selinger and Hartzog’s view, the solution to this lack of “consentability” and the failure of procedural requirements for government uses is to ban the technology.

The European Commission’s recently proposed Artificial Intelligence Act, which is currently under consideration by EU member states and would encompass facial recognition technology, notably does not rely on a notice and consent framework.<sup>76</sup> Rather the AI Act takes a risk-based approach to regulation, with uses that pose an unacceptable risk being banned and uses with minimal or no risk being permitted with no restrictions. In the middle there are high-risk uses that are permitted subject to compliance with specific substantive requirements and an ex-ante conformity assessment and AI uses that are permitted but subject to information/transparency obligations. In its current form, the draft AI Act prohibits the use of AI systems for “real-time” remote biometric identification (e.g., facial recognition for identification) of persons in publicly available spaces for the purpose of law enforcement.<sup>77</sup> This is because it is “considered particularly intrusive to the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights.”<sup>78</sup> An exception to this general prohibition is where the use of the system is necessary to achieve a substantial public interest, the importance of which outweighs the risks.<sup>79</sup> Those situations involve the search for potential victims of crime, including missing children; certain threats to the life or physical safety of natural persons or of a terrorist attack; and the detection, localization, identification or prosecution of perpetrators or suspects of certain criminal offences.<sup>80</sup>

---

<sup>70</sup> Evan Selinger & Woodrow Hartzog, 66 LOYOLA LAW REVIEW, at 101, 114-15 (2020).

<sup>71</sup> *Id.* at 116.

<sup>72</sup> *Id.*

<sup>73</sup> *Id.*

<sup>74</sup> *Id.*

<sup>75</sup> *Id.*

<sup>76</sup> European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, 2021/0106 (COD) (“AI Act”).

<sup>77</sup> *Id.* at Article 5.1(d).

<sup>78</sup> *Id.* at Preamble, (18).

<sup>79</sup> *Id.* at Article 5.1(d).

<sup>80</sup> *Id.*



In sum, there are arguments that a shift away from reliance on notice and consent principles is needed given that the prevalence of digital technologies in our daily lives has complicated the ability for entities to provide transparent notice and obtain informed consent. These considerations are amplified for facial recognition technology because of the increased pervasiveness of the technology and the potential for abuse without substantive protections in place. Something other than notice and consent may be necessary given the potential of the use of the technology to harm individuals and harm to our democratic norms writ large. Policymakers and legislators who are charged with regulating facial recognition technology will want to take these considerations in account. In particular, they will want to be cognizant of when a reliance on pure notice and consent principles can be compatible with facial recognition technology, or whether some other means of regulating the technology would better serve individuals and society.

## VII. PRINCIPLES

### A. Principle 1: Legislators and policymakers should recognize the limitations of notice and consent for facial recognition technology

Legislators and policymakers should acknowledge the limitations of notice and consent, especially in the current landscape where people are faced with an avalanche of notice and consent requests of varying levels of utility. These requests are often of minimal value; they are either too detailed or are reduced to superficial warnings and are largely ignored by most people. As such, they are neither informative nor privacy protective. As explained above in Section VI, a general recognition of the shortcomings of notice and consent is causing a reassessment of whether it should be relied on as a basis for processing personal information, or whether something more (or something else) is required to ensure adequate protection for certain technology uses.

Against this backdrop, legislators and policymakers will want to think about whether all uses of facial recognition technology are the same, and therefore should be regulated in the same manner, or whether certain uses might merit different treatment. Are there scenarios in which notice and consent can be used as a legal framework for facial recognition technology, and are there other scenarios where it cannot? Consideration should be given to the risk posed by the particular application weighed against its benefits, whether it is a “worthwhile” use (recognizing there is an implicit value judgment being made in such an approach), as well as the practicality of providing adequate notice and consent given the circumstances of the particular use.

In circumstances where the risk of the particular application is higher, notice and consent might not be appropriate for a number of reasons. A high-risk application might be one that poses significant risks to the health and safety or fundamental rights of people regardless of any benefits conferred.<sup>81</sup> For example, the use of real time facial recognition identification in a public place would be considered high risk because of the potential for surveillance, to chill speech, and to infringe on civil liberties. Where the risks of a particular use are high, it might not be possible to efficiently and fully present in a notice all the risks in a transparent manner, or in a way that ensures people will even see the notice and assess its contents. Where adequate notice is not provided, then consent cannot be informed. There may also be scenarios in which the high risk posed by the technology requires that the individual take an affirmative action that clearly and unmistakably evidences their intent to be subject to the technology. The use of facial recognition technology for

---

<sup>81</sup> See AI Act.

real time monitoring in a public place is a situation where notice and consent would be difficult to perfect. A simple sign with a camera on it that says the location is subject to real time use of facial recognition technology does not provide individuals with sufficient information to assess the risks. And simply choosing to remain in a public location where real time facial recognition technology is being used, should not be sufficient to convey informed consent, especially given a person's need to access public locations, and the difficulties around providing notice in such a location.

There might also be applications where the benefits of the particular use are marginal and therefore do not justify the use of the technology. For example, legislators and policymakers should consider whether there are particular uses that provide minimal benefits and should be discouraged, perhaps because the use can be achieved through a less intrusive technical means with similar results. This could involve an analysis similar to what is required under the GDPR of whether the use of facial recognition technology is necessary and whether it is proportionate to the intended aim. An example of this could be the use of facial recognition technology to market to people in a store over time and across visits. A grocery store or other retailer could theoretically capture an image of a person's face upon checkout at one visit, and then use that information to market to them on subsequent visits to the store. This might be the type of low value / low benefit use that legislators and policymakers could decide merits special treatment, whether that is through prohibiting its use or through substantive protections that guard against concerns like surveillance and discrimination.

## **B. Principle 2: Notice and consent can be compatible with lower risk uses of facial recognition technology**

Policymakers and legislators will want to consider whether there are certain lower risk uses of facial recognition technology that are “compatible with” a notice and consent framework, i.e., the risks of the uses when weighed against the benefits of the uses are such that they are sufficiently addressed by a notice and consent framework and need not be subjected to direct substantive limitations. Lower risk uses are compatible with notice and consent because less has to be disclosed in order to fully inform an individual about the potential risks, and because the threshold needed to achieve informed consent will likely be lower.

One potential way to distinguish a higher risk from lower risk use is to think about whether the ultimate purpose is verification/authentication versus identification. The differences between the two may mean that they merit different treatment. As described earlier, verification uses—or one to one matching—are when the technology is used to match a pre-existing image in a gallery database against the specific image of an individual who is presenting themselves for a particular purpose. The identification of the individual is not needed for this match to occur; the fact of the match is sufficient. Identification uses—or one-to-many matching—is when the ultimate purpose is to identify the person who is presenting themselves for an image (or appears in an image), by comparing that person against a gallery of presumably known individuals. Although there are certainly risks posed by any use of facial recognition technology (as is true for most digital technologies), risks relating to surveillance, a loss of obscurity, and broader societal harms are primarily present with identification uses. Despite slippery slope arguments that there is fundamentally no difference between verification uses and identification uses because the technology underlying those systems is the same, consideration should be given as to whether that alone means that they merit similar treatment, or if there are guardrails that can be put around verification uses to protect against such harms.



Another reason for treating verification and identification uses differently, beyond the risks posed by each, is that obtaining notice and consent may not be realistic for many identification uses. In the verification uses that the drafting team considered, there is typically a relationship between the entity using facial recognition technology and the person who is subject to it. Verification uses provide some opportunity for the collecting entity to meaningfully interact with the individual whose biometric data is being collected. For example, the most commonly known verification uses involve a person whose image is captured and stored in their smartphone so that it can later be matched against another image taken, later in time, of that same person to open the device or access a particular feature on the device. In such a scenario, the relationship between the two parties makes the potential for meaningful notice possible, for questions to be asked, and for consent to be obtained both at the time of gallery image capture and when the person presents themselves for verification. In addition, surveillance concerns are lessened where reference images have been gathered for a specific (and, presumably, limited purpose) and where individuals know that their data has been collected for the purpose.

Identification uses do not necessarily require that such a relationship be present. Facial recognition technology can be used on people in a surreptitious manner for identification purposes. Databases used for identification can be compiled from any number of sources where there is not a direct relationship between the data subject and the entity using facial recognition technology. The Clearview AI database was built almost entirely from images scraped from websites, and many government databases are built from data obtained from numerous sources, including private entities like Clearview AI as well as drivers' license photos from state departments of motor vehicles.<sup>82</sup> Even assuming that an individual might have received notice and consented to the capture of an image that will be used to match against a gallery, that does not necessarily mean that they either know or consented to the use of their image to be placed in that gallery to be used later in time for an identification purpose. The fear, in this scenario, is therefore not only that images may unknowingly be collected for the gallery, but that the image to be matched will also be surreptitiously collected. In other words, the risk of unfair collection in identification uses can occur at both ends of the equation, a risk that is heightened by the potential for there to be no direct relationship between the person and the entity using the technology.

Legislators and policymakers will also want to think about whether there are differences between lower risk public sector uses and lower risk private sector uses such that they merit different treatment. As a general matter, so long as the notice is transparent and consent is informed and substantive limitations are in place where and to the extent they are found to be appropriate (as described in more detail in Section VII.D, below), the authors of this commentary believe the ability to rely on notice and consent as a basis for employing facial recognition technology for lower risk uses should not be affected by whether the use is by the public or private sector.

### **C. Principle 3: Where required, notice should be meaningful and consent should be informed**

To the extent that legislators and policymakers rely on notice and consent in regulating facial recognition technology, the required notice should be meaningful and the required consent should be informed. Although what makes a notice meaningful and consent informed will vary with the

---

<sup>82</sup> See Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020).

particular circumstances, there are a few foundational elements that legislators and policymakers will want to consider for any regulatory scheme that requires notice and consent in connection with employing facial recognition technology.

## 1. Notice

Where entities are using facial recognition technology for lower risk uses (e.g., verification), those entities must provide transparency around their data practices. The notice should be meaningful.<sup>83</sup> There are three elements that are necessary for notice to be meaningful: timing, presentation, and content:

- *Timing.* The presentation of the notice should be timed so that people understand the importance of the content and tie it to the decision that they are being asked to make. The notice must be given prior to the capture of the facial image that will be used as the reference image in the gallery image database. This is to ensure that the individual is given the opportunity to understand why their data is being captured in the first place and so that they can make an informed decision.<sup>84</sup> The timing of the notice is also important to minimize coercion of the individual. For example, entities should present the notice 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 meant to ensure 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.
- *Presentation.* The visual presentation of the notice should be such that the purpose and meaning of the notice is unambiguous. The notice should be clearly understandable to the average person and should be independent from other disclosures, for example, other legal or financial disclosures.<sup>85</sup>
- *Content.* The notice needs to provide enough information so that a person understands what they are agreeing to and to allow them to assess the tradeoff they are being asked to make. At a minimum this means that it should explain why their image is being collected, and how it will be used. The notice should also explain which entities will have access to the biometric information and/or with whom it will be shared, and for what purposes, including whether it may be shared with law enforcement, and under what circumstances that might occur. The notice should either link to the entity's privacy policy or explain where that privacy policy can be accessed, and should provide contact information for a resource that can answer any questions the individual might have about the collection and use of his or her data.

---

<sup>83</sup> In defining what constitutes meaningful notice, the drafting team analyzed various existing statutes regulating biometrics and privacy more generally.

<sup>84</sup> 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).

<sup>85</sup> 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).

## 2. Consent

In addition to providing proper notice, entities relying on notice and consent as a basis for collecting data must ensure that the consent obtained is informed. Legislators and policymakers will want to take into account the following considerations when determining what constitutes adequate consent for verification and other lower risk uses of facial recognition technology.

### a. *Consent should be timed properly*

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 verification purposes.<sup>86</sup> 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.<sup>87</sup>

### b. *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 consenting, and understand the consequences of their decision. 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).

### c. *Consent should be express*

Given the special risks posed by facial recognition technology, consent should 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 verification 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, knowingly standing still for a photograph that will be later used as a reference image—but the main distinction is that

---

<sup>86</sup> 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).

<sup>87</sup> 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).

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).<sup>88</sup>

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. Effective express consent, however, 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, the duration of the use, 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. 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.

d. *Consent should be freely given*

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. 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. Another effective way of ensuring that consent is freely given is to provide an alternative means of obtaining the same access or benefit. This is particularly helpful—and workable—facial recognition is used for verification. For example, allowing a user of a secure service to verify their identity by providing a less intrusive biometric (e.g., fingerprint) or a username/password instead of a facial scan would make any consent obtained more clearly voluntary instead of coerced.

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” for verification and that

---

<sup>88</sup> 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).

consumers are induced to consent in exchange for discounts. Without the facial recognition incentive, the business may set above-market food prices. In that situation, the only way for the consumer to obtain “reasonable” food prices would be to consent to facial recognition given the consumer’s lack of access to alternative venues. This implementation may be considered unduly coercive both because the consumer does not have any meaningful choice, and the products at issue are necessities. In this “take it or leave it” consent regime, individuals may feel that they are being pressured to make a choice in order to obtain an otherwise unavailable product or service.

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.<sup>89</sup> 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.

e. *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.<sup>90</sup> However, the “right to be forgotten,” as embodied in the General Data Protection Regulation<sup>91</sup> and statutes such as California’s Consumer Privacy Act and Privacy Rights Act,<sup>92</sup> 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.<sup>93</sup>

<sup>89</sup> Under the CPRA, consent cannot be obtained through dark patterns. Cal. Civ. Code § 1798.140(h).

<sup>90</sup> 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.

<sup>91</sup> See generally GDPR Article 17, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e2606-1-1>.

<sup>92</sup> Cal. Civ. Code s. 1798.105, [https://leginfo.ca.gov/faces/codes\\_displaySection.xhtml?sectionNum=1798.105.&nodeTreePath=8.4.45&lawCode=CIV](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](https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf).

<sup>93</sup> 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.



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 often system developers, themselves, do not entirely understand the exact details of how data is actually used to train a particular facial recognition AI algorithm (artificial neural networks in particular). This lack 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.<sup>94</sup> 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.<sup>95</sup>

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.<sup>96</sup> There is generally a massive amount of technological overhead involved in the ingesting and training process, such that 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.

---

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).

<sup>94</sup> 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 involves 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 or recreating 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 in a “deanonymization”/“reidentification” attack to match data with particular named people in the community, by making 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](https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1816&context=faculty_scholarship).

<sup>95</sup> *Id.*

<sup>96</sup> 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](https://scholarship.law.bu.edu/faculty_scholarship/817).

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.

#### **D. Principle 4: Substantive limitations offer important protections, even for lower risk uses**

Although concerns relating to surveillance are lessened for verification and other lower risk uses of the technology, the potential for harms to individual privacy and civil liberties as well as data misuse are not absent. Therefore, even where procedural protections like notice and consent are implemented for verification and other lower risk uses, policymakers and legislatures must consider what additional substantive limitations on the collection of biometric data and its use for facial recognition are also needed in order to sufficiently protect individuals. Notice and consent, without substantive limitations, may never be enough for certain types of verification uses to adequately protect individuals given the potential risks attendant with facial recognition technology, and the potential for data originally collected for a verification purpose to be misused in some fashion after collection. For example, to guard against data being collected for verification purposes, but then later being used for identification purposes where notice and consent have not been obtained. In addition, substantive limitations help ensure that there is adequate protection in the event that the notice provided was somehow inadequate or that the consent obtained was somehow not informed.

Although there are a number of potential substantive limitations that could be considered, there are certain baseline protections that legislators and policymakers will want to consider to ensure that individuals' data and civil liberties are adequately protected. These are a purpose limitation and data security. In addition to implementing these guardrails, legislators will also want to consider whether there are additional substantive limitations that might be required given the risks posed by any particular use.

##### **1. Purpose Limitation**

A purpose limitation prohibits secondary uses of collected data (i.e., uses that are materially different from the use for which the data was collected. For example, if a facial image is captured in order to verify that the individual making a purchase is the same person who holds an account from which payment will be made, that biometric data—either the gallery image or the query image—can only be used to verify that the image is a match. It could not be used, for example, for marketing purposes or used in an identification database. And it certainly could not be sold or transferred so that another entity could make use of the data for purposes that were beyond the scope of the original purpose. However, legislators and policymakers may want to make allowances for entities to use biometric information in the possession of third parties for law enforcement purposes where there are due process protections in place, the use is limited, and there are additional restrictions placed on the downstream use of such information. For example, the IL BIPA and Texas's Capture or Use of Biometric Identifier Act ("CUBI") law prohibit the disclosure of commercial biometric data to law enforcement unless it is disclosed pursuant to (or "in response to") a warrant or subpoena.<sup>97</sup> Such a limitation helps protect against harms attendant to the use of facial recognition technology, while also allowing for some secondary uses that may be in the public interest.

---

<sup>97</sup> Tex. Bus. and Comm. Code s. 503.001(c); 740 ILCS 14/15(d). Even in states that permit sharing of this information without a warrant, it may be appropriate to require notice when such sharing has voluntarily occurred, particularly when



In recognizing that a purpose limitation is important, legislators and policymakers should recognize that the strictest view of a purpose limitation should not necessarily be taken. Attendant uses that are needed to support the provision of the verification service should also be permitted. For example, using images to train a model and for troubleshooting can be reasonably considered a use for the purpose of providing the services.

## 2. Reasonable Data Security

As explained above, any use of facial recognition technology comes with some degree of risk. What happens when an individual's facial geometry or other biometric data is acquired by an unauthorized third party? The bad actor gains access to a highly trusted key that could open up access to the individual's financial accounts and devices.<sup>98</sup> The risk of a data breach demonstrates the need to protect the underlying biometric data.<sup>99</sup>

Despite these risks and the ever-increasing prevalence of both malicious and inadvertent data breaches, privacy and data security laws have been slow to account for biometric data. Even

---

notice would not compromise ongoing law enforcement activities. While an earlier Washington statute that pertained solely to use of facial recognition systems by the state's department of (vehicle) licensing ("DOL") (and prohibited disclosure of facial recognition data except pursuant to court order, or solely to establish a criminal offense comprising fraudulent use or creation of a real or bogus Washington driver's license or ID (RCW 43.386.100); Washington State's later "commercial purpose" statute, which was passed around the same time as the Illinois and Texas laws expressly did not address use by law enforcement ([RCW 19.375.040\(3\)](#)), although it provides that a subject's biometric identifier may be disclosed for a commercial purpose (sic) without the subject's consent, if authorized by a court order, or to respond or participate in judicial process (RCW 19.375.020(3)(d, f). A later Washington statute, [RCW 43.386](#) et seq., however, restricted the use of facial recognition by law enforcement (43.386.080), and requires judicial (43.386.070(3) and law enforcement (43.386.070(4) reporting of law enforcement warrant applications for use of facial recognition in surveillance. The law further provides that use of a facial recognition service be disclosed to a criminal defendant prior to trial (RCW 43.386.070(1)), and requires that non-DOL\* state agencies must provide a legislative authority with notice of intent to use a facial recognition system, specifying the purpose, and producing an accountability report for the service (RCW 43.386.020); and requires operational and bias testing (RCW 43.386.040, .050). <https://lawfilesexternal.wa.gov/biennium/2019-20/Pdf/Bills/Session%20Laws/Senate/6280-S.L.pdf?q=20200722075210>.

\* As noted above, Washington's department of [vehicle] licensing was already subject to a separate facial recognition statute cited in the 2020 law ( 46.20.037, cited in RCW 43.386.100); the earlier law provides that: the department's may only be used to verify the identity of an applicant for a license or ID in order to determine whether they have been previously issued a license or ID (RCW 46.20.037(1); and the department must post conspicuous notices regarding the use of the system in department licensing offices and make written specified information about the system available on the department's website. (RCW 46.20.037(3).

<sup>98</sup> Unlike other types of sensitive personal information, it is difficult to remediate the potential damage caused by compromised biometric data. The Illinois legislature recognized this within the text of BIPA by stating: "Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." 740 Ill. Comp. Stat. Ann. 14/5(c). *See also* GAO Report, *Facial Recognition Technology - Commercial Uses, Privacy Issues, and Applicable Federal Law*, at 16 (July 2015).

<sup>99</sup> Unfortunately, these risks are not merely hypothetical. Already there have already been several high-profile data breaches that have compromised individuals' biometric data. For example, in 2019, the U.S. Customs and Border Protection (CBP) disclosed a vendor data breach involving individuals' photographs and driver's license images that impacted approximately 100,000 individuals. Drew Harwell and Geoffrey Fowler, *U.S. Customs and Border Protection Says Photos of Travelers Were Taken in a Data Breach*, WASH. POST (June 10, 2019), available at <https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/>. As a result of the incident, at least a portion of these individuals' data was offered for sale on the dark web.

the biometric-specific laws in Illinois, Texas, and Washington contain only general high-level security requirements for biometric data.<sup>100</sup> For example, BIPA requires entities in possession of biometric data to “store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity’s industry.” However, the majority of states have few to no requirements or standards surrounding the protection of biometric data, even though an increasing number of state data breach notification laws include biometric information, or some derivation of that term, within the definition of triggering “personal information.”<sup>101</sup> With the approaching effective dates of the California Privacy Rights Act (CPRA), Virginia Consumer Data Protection Act (CDPA), and Colorado Privacy Act (CPA), each of which include biometric data within the definition of “personal information,” companies operating in those states will have at least a baseline requirement to maintain reasonable administrative, technical, and physical data security practices.

Given the potential risk of harm associated with the loss or misuse of an individual’s biometric data, these gaps should be closed and any entity collecting or using biometric data should be subject to sensible data security standards that are both commercially reasonable and appropriate to the risk.<sup>102</sup> However, given the uniqueness of biometric data for the reasons set forth above, legislatures should choose to go above and beyond a generic reasonableness standard. Specific to biometric data, legislatures may also choose more detailed or proscriptive security controls, three of which are outlined below.

- First, one of the most common security mechanisms available to protect facial geometries is to segregate any biometric data from other types of personally identifiable information.<sup>103</sup> Using this method, the data is stored as an encrypted digital template as opposed to a raw original image.<sup>104</sup> While the inherent identifying nature of biometric data would not render this data entirely secure or incapable of identifying an individual, this method creates a firewall that would require additional steps and analysis before being rendered in a usable state by a third party. Because “[e]ach developer measures and records [biometric] templates differently” this step provides “an additional layer of security by making this data useless if compromised, either for identification or as a credential outside of the system that created it.”<sup>105</sup>
- Second and perhaps most obviously, given the highly sensitive nature of biometric data, facial geometries should be encrypted throughout the life cycle of the data, including

<sup>100</sup> 740 Ill. Comp. Stat. Ann. 14/15(e)(1).

<sup>101</sup> See, e.g., Cal. Civ. Code § 1798.82(h)(1)(f) (“Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.”).

<sup>102</sup> See, e.g., FTC, Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission, June 13, 2020, available at (“[C]ompanies should employ reasonable security to protect consumer data.”).

<sup>103</sup> GAO, Facial Recognition Technology - Commercial Uses, Privacy Issues, and Applicable Federal Law at 25 (July 2015).

<sup>104</sup> Note that, even in this context, the underlying image should be adequately protected as well. See FTC, Best Practices for Common Uses of Facial Recognition Technologies at 12 (October 2012).

<sup>105</sup> Security Industry Association, SIA Principles for the Responsible and Effective Use of Facial Recognition Technology (August 2020) available at <https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/>.

both at rest and in motion.<sup>106</sup> Best practices are developing which rely on new encryption technologies to protect the security of face representations including fully homomorphic encryption.

- Third, an alternative option is found in BIPA, which does not use a tiered approach, but requires the development of “a written policy . . . establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.”<sup>107</sup> This written policy requirement could be expanded to include a written information security program targeted to protect facial recognition data.

#### **E. Principle 5: Notice and consent offer insufficient protection for higher risk uses**

Policymakers and legislators should recognize that there are certain uses of facial recognition technology that are higher risk. Facial recognition technology is unique in its potential to be used for mass surveillance, both by government actors and private companies. Many of the more significant harms that critics of the technology have focused on are grounded in concerns about the potential for real-time monitoring and a loss of personal obscurity. There is also the potential for certain uses to result in an erosion of civil liberties and civil rights, including a right to due process and freedom of association and expression. For the most part, these types of risks relate to the use of the technology for identification purposes, especially in real time, and frequently by government actors. Although there may be certain benefits to using the technology for identification purposes, the risks are substantial enough that legislators and policymakers must approach regulation in this area cautiously and with a recognition that the types of longer-term harms that come with a pervasive surveillance are at present still difficult to foresee and quantify. In addition, short term trade-offs that are made for convenience and efficiency may be difficult to unwind once the damage has been done.

The potential for harm when facial recognition is used for identification purposes, even given the benefits that may come from it, makes it the kind of higher-risk use that requires that legislators and policymakers to look beyond notice and consent as a basis for regulating the technology. That is because it is very unlikely that notice and consent can be perfected for a high risk use like identification. With regard to notice, it is difficult to conceive of a description of facial recognition technology for identification purposes that could succinctly, and in an understandable manner, inform an individual about the potential harm attendant with its use. In addition, especially for public places, there are certainly difficulties with ensuring that each individual will even see the notice, not to mention take the time to review its contents. Legislators and policymakers should also question whether consent can ever be informed given the problems with providing adequate notice, and where one's consent not only has implications for their own personal autonomy, but for the rights of all others in the community.

---

<sup>106</sup> See, e.g., International Biometrics & Identification Association, Principles for Biometric Data Security and Privacy at 6 (August 2019).

<sup>107</sup> 740 Ill. Comp. Stat. Ann. 14/15(a).

Accepting the premise that notice and consent is not the proper conceptual framework for thinking about how to regulate identification and other high-risk uses of facial recognition, then there are two approaches that legislators and policymakers can take. One path, which has been taken in many jurisdictions, is to prohibit the use of the technology outright.<sup>108</sup> This implicitly acknowledges that notice and consent do not offer appropriate protections, and that in the absence of an alternative framework, then the only responsible approach is to ban its use altogether. The second path asks whether there are substantive protections that can be put in place to sufficiently guard against the risks of using the technology such that we as a society are willing to benefit from the use of the technology.

For some identification uses, legislators and policymakers will be able to craft conditions that permit the use of the technology in a manner that implements sufficient guardrails around its use. At a minimum, these would need to include the substantive limitations described above in Section VII.D. However, additional measures will need to be implemented to ensure that those deploying the technology are held to transparency and accountability standards. One way to think about transparency and accountability is 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 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 prior to deployment, 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 or some other 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, government contractor, or where the use may ultimately affect the public.

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, entity leadership, and administrative arbiters to assess whether the conditions and manner of use are acceptable. Legislators and policymakers should require that 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.

---

<sup>108</sup> See discussion state and local moratoriums in Section I.V. and the AI Act's approach to regulating real-time use of facial recognition technology for law enforcement purposes in public places in Section VI., *supra*.

- 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.<sup>109</sup>
- 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.

---

<sup>109</sup> 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 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.



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 is 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 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 evidence generated by the technology and guard against injustice.

## Appendix A:<sup>110</sup>

### 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), and prevents the disclosure of customer biometric data without customer consent, subject to limited exceptions including disclosure to law enforcement pursuant to a valid warrant. 740 ILL COMP. STAT. 14/15(d). 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

---

<sup>110</sup> 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 numerous police processing activities of footage from BWC, “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. Biometric data captured for a commercial purpose must be stored, transmitted, and protected using “reasonable care,” and may not be sold, leased or disclosed without consent subject to limited exceptions including disclosure to law enforcement pursuant to warrant. 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. The ban 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 only 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.
- **Pennsylvania**
  - **City of Pittsburgh.** The City of Pittsburgh City Council voted in September 2020 to regulate the use of facial recognition and predictive policing technologies by city entities, including the Pittsburgh Bureau of Police. The legislation requires city council approval of such technologies before they are acquired or used, except in "an emergency situation."
- **Washington**

- **King County, Washington.** King County, Washington, which includes 2.3 million people in and around Seattle, passed an ordinance banning the use of FRT in June 2021.
- **Wisconsin**
  - **City of Madison.** In December 2020, Madison city council voted to ban use of FRT by government entities. 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 Act of 2022](#) would place limits on law enforcement use of facial recognition technology, including limiting its use to situations when a warrant is obtained that show probable cause that an individual committed a serious violent felony. It would also prohibit law enforcement use in conjunction with databases that contain illegitimately obtained information and body cameras, dashboard cameras, and aircraft cameras, and to track individuals with live or stored video footage. The bill also includes transparency provisions, such as providing notice to individuals who are subjects of a facial recognition search and a copy of the court order and/or other key data points, and requires regular auditing and independent testing of facial recognition technology systems.
- 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.

## 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.<sup>111</sup> 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.”<sup>112</sup> The notice and consent principle state 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.”<sup>113</sup> 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.”<sup>114</sup>
- The FTC issued recommended best practices for facial recognition technology in its *Best Practices for Common Uses of Facial Recognition Technologies* staff report.<sup>115</sup> 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.<sup>116</sup> The FTC also emphasized the need for simplified consumer choice and transparency. The report generally advocates that consumers be presented with clear notice about how the facial recognition features work, what data will be collected, and how that data will be used.<sup>117</sup> The report also recommends providing consumers with a

---

<sup>111</sup> 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](http://www3.weforum.org/docs/WEF_Framework_for_action_Facial_recognition_2020.pdf). The first version of the principles is part of a larger multi-stakeholder effort to define the responsible use of facial recognition, and is intended to be reviewed and updated based on an 18-month pilot project.

<sup>112</sup> *Id.* at 8.

<sup>113</sup> *Id.*

<sup>114</sup> *Id.*

<sup>115</sup> 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.

<sup>116</sup> *Id.* at ii.

<sup>117</sup> *Id.*

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.<sup>118</sup> The FTC report also envisions affirmative express consent being necessary in two scenarios.<sup>119</sup> 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.<sup>120</sup> 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.”<sup>121</sup> 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.<sup>122</sup> Although these principles do envision covered entities providing notice to consumers, they do not provide consumers with any meaningful choice. There is no ability to opt out or requirement that consumers consent in any meaningful way. When covered entities make material changes to their facial template data management practices, the principles encourage them to update their policies or disclosures, though affirmative express consent is not required.<sup>123</sup> The use limitation

---

<sup>118</sup> *Id.*

<sup>119</sup> 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.

<sup>120</sup> 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](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/](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.

<sup>121</sup> NTIA Privacy Best Practice Recommendations for Commercial Facial Recognition Use, *supra* note 95 at 2.

<sup>122</sup> *Id.* at 2.

<sup>123</sup> *Id.* at 2.

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*.<sup>124</sup> 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.”<sup>125</sup> 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.<sup>126</sup> 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.<sup>127</sup> 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.<sup>128</sup> The principles also state that companies implementing facial recognition systems should provide consumers with meaningful notice about how the facial recognition software templates are created and how such data will be used, stored, shared, and maintained. The principles explain that, among other things, the notice should help consumers understand the purposes of the collection, whether the data may be shared, retention, deletion, or de-identification policies for facial recognition data, choices consumers may have, and which third-party partners receive the data.<sup>129</sup> 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.<sup>130</sup>

---

<sup>124</sup> 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 “intended to set industry best practices, inform consumer expectations, and educate policymakers.” *Id.* at 1.

<sup>125</sup> *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.

<sup>126</sup> *Id.* at 3.

<sup>127</sup> *Id.* at 4.

<sup>128</sup> *Id.* at 4.

<sup>129</sup> *Id.* at 6.

<sup>130</sup> *Id.* at 6.