LET'S "FACE" IT: FACIAL RECOGNITION TECHNOLOGY, POLICE SURVEILLANCE, AND THE CONSTITUTION

Melanie A. Bigos[*]

I. Introduction

Governmental surveillance through artificial intelligence was once portrayed as a dystopian practice, reserved for science fiction films and novels.[1] The reality today is that one in two American adults have been subjected to inclusion in a law enforcement face recognition network.[2] The rapid development of such technology in recent years enables police to effectively collect and analyze biometric data for

[*] J.D. Candidate, Suffolk University Law School, 2022; B.A. in Psychology, Boston College, 2019. Melanie can be reached at melaniebigos@gmail.com.

[1] *See* John W. Whitehead, *The Omnipresent Surveillance State: Orwell's 1984 Is No Longer Fiction*, RIVER CITIES' READER (June 10, 2019), *archived at* https://perma.cc/7MT8-VTW3 (noting the similarities between contemporary government surveillance and that which is depicted in George Orwell's 1948 dystopian novel, *1984*, where "advanced technology has become the driving force behind a surveillance-driven society"); Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology,* 49 CONN. L. REV. 1591, 1594 (2017) (citing the 2002 film *Minority Report*, where extreme surveillance via facial recognition blocks independent thought). "Despite the deep unease at the world of prevalent facial recognition, we continue to inch closer to that reality without an adequate discussion of the consequences." Hirose, *supra*.

[2] *See* CLARE GARVIE ET AL., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 1 (Oct. 18, 2016), *archived at* https://perma.cc/29AV-28JJ (delineating law enforcement's widespread yet surreptitious use of facial recognition systems in the United States).

surveillance purposes.[3] Specifically, facial recognition technology empowers law enforcement to identify individual faces, whether it be within a large crowd or in a photoset.[4] Access to this powerful and efficient technology heralds a massive evolution in law enforcement's procedural methods and signifies a vast increase in information at the government's fingertips.[5] Implementation of this extensive surveillance technology, however, is at great odds with society's growing concerns regarding the capricious power dynamic between police authority and individual freedoms.[6]

[3] *See* Jon Schuppe, *How facial recognition became a routine policing tool in America*, NBC NEWS (May 11, 2019), *archived at* https://perma.cc/R54H-8YUL (describing the technology-driven revolution in policing and citing the technology's ease of operation for police forces). *See also* Kirill Levashov, *THE RISE OF A NEW TYPE OF SURVEILLANCE FOR WHICH THE LAW WASN'T READY*, 15 COLUM. SCI. & TECH. L. REV. 164, 167 (2013) (outlining the prominence of facial recognition strategies in policing and how this practice is largely unregulated, raising concerns regarding privacy, security, and free association). *See, e.g.*, Aris Folley, *Memphis Police store secret surveillance of Black Lives Matter protesters for 'watch list'*, AOL (Feb. 21, 2017), *archived at* https://perma.cc/DR2F-BL9V (providing an example of government surveillance with the Memphis police department's creation of a "watch list" of individuals participating in protests); Drew Harwell & Craig Timberg, *How America's surveillance networks helped the FBI catch the Capitol mob*, THE WASH. POST (Apr. 2, 2021), *archived at* https://perma.cc/X8TL-X2VZ (detailing the government's access to a variety of surveillance tactics (including facial recognition) used to identify those present at the January 6, 2021 Capitol riots).

[4] *See* GARVIE ET AL., *supra* note 2 at 10 (explaining the complex methods of identification that are afforded to law enforcement agencies); Thorin Klosowski, *Facial Recognition is Everywhere. Here's What We Can Do About It.*, WIRECUTTER (July 15, 2020), *archived at* https://perma.cc/9TMX-4Q7G (explaining how government agencies may use facial recognition surveillance to identify faces in a large crowd or may alternatively use it to compare faces to those in a photo database, for instance).

[5] *See* Katelyn Ringrose, *LAW ENFORCEMENT'S PAIRING OF FACIAL RECOGNITION TECHNOLOGY WITH BODY-WORN CAMERAS ESCALATES PRIVACY CONCERNS*, 105 VA. L. REV. ONLINE 57, 57 (2019) (suggesting that police use of facial recognition technology, especially in conjunction with body-worn cameras, is a dangerous method of mass surveillance); Neena Singh Guliani, *The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database*, ACLU (June 7, 2019), *archived at* https://perma.cc/FB3Q-RQN2 (recognizing the massive database of photos, such as those from driver's licenses, which the FBI can access). As of 2019, this number was at approximately 640 million photos, and expanding rapidly—a number that exceeds the total population of the United States. Guliani, *supra*.

[6] *See* GARVIE ET AL., *supra* note 2, at 8 (describing society's growing concerns with widespread police authority).

While Apple's iPhone and Facebook's tagging feature familiarized the world with facial recognition technologies through their commercial implementation, law enforcement's usage is more surreptitious in nature—and spreading rapidly.[7] One estimate predicts that the market for facial recognition technology in federal, state, and local law enforcement will reach $375 million by 2025, an increase from $136.9 million in 2018.[8] Additionally, the Center on Privacy & Technology at Georgetown Law School approximates that one in four police departments utilize facial recognition technology.[9] Further intensifying the pushback against governmental implementation of facial recognition systems is the potential for abuse or discrimination that can result from algorithm biases.[10] A 2019 study conducted by

[7] *See* Lindsey Barrett, *BAN FACIAL RECOGNITION TECHNOLOGIES FOR CHILDREN? AND FOR EVERYONE ELSE*, 26 B.U. J. SCI. & TECH. L. 223, 236 (2020) (claiming that use of facial recognition technologies by the government tend to be "even more coercive and surreptitious than commercial ones, and often have more severe implications due to the authority the governmental entity might have, and the context in which the technology is used."); Sharon Nakar & Dov Greenbaum, *NOW YOU SEE ME. NOW YOU STILL DO: FACIAL RECOGNITION TECHNOLOGY AND THE GROWING LACK OF PRIVACY*, 23 B.U. J. SCI. & TECH. L. 88, 93 (2017) (marking the lack of public knowledge as the most disconcerting element of facial recognition's use).

[8] *See* Schuppe, *supra* note 3 (describing the vast expectancy of growth in the market for facial recognition technology). The potential proliferation for this use may be driven in part by its cost-effectiveness: its use requires little overhead, unlike costly and time-consuming technologies such as DNA evidence. *Id.*

[9] *See* GARVIE ET AL., *supra* note 2, at 25 (estimating that "more than one in four of all American state and local law enforcement agencies can run face recognition searches of their own databases, run those searches on another agency's face recognition system, or have the option to access such a system."). Approximately 5,300 government officials from 242 different federal, state, and local agencies can access these databases. *Id.* These databases are accessible by several government agencies, including but not limited to, the Department of Defense, the Drug Enforcement Administration, Immigration and Customs Enforcement, the Internal Revenue Service, the Social Security Administration, the U.S. Air Force Office of Special Investigations, and the U.S. Marshals Service. *Id.*

[10] *See* Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use*, THE WASH. POST (Dec. 19, 2019), *archived at* https://perma.cc/BK9X-5P4H (outlining the 2019 study conducted by the National Institute of Standards and Technology (NIST) which revealed lapses in the algorithms of the majority of facial recognition software in the industry); Sahil Chinoy, *The Racist History Behind Facial Recognition*, THE N.Y. TIMES (July 10, 2019), *archived at* https://perma.cc/96LA-R8ST (dissecting the categorical nature of most algorithms which creates several inconsistencies in facial recognition among different ethnic groups); Steve Lohr, *Facial Recognition is Accurate, if You're a*

the National Institute of Standards and Technology ("NIST") evaluated 189 different software algorithms—representing a majority of the industry—and determined that most systems misidentify people of color at a higher frequency than Caucasians.[11] This high error rate, in conjunction with other privacy concerns, has led several American cities to ban government use of such facial recognition technology.[12]

White Guy, THE N.Y. TIMES (Feb. 9, 2018), *archived at* https://perma.cc/5PXH-CVTJ (explaining that facial recognition systems rely on large and diverse datasets for accuracy and tend to be less accurate for minority groups).

[11] *See* Patrick Grother et al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Test*, NIST INTERAGENCY INTERN. REP. 8280 (2019) (reporting the high error rates of most facial recognition algorithms). *See also* Drew Harwell, *Amazon facial-identification software used by police falls short on tests for accuracy and bias, new research finds*, THE WASH. POST (Jan. 25, 2019), *archived at* https://perma.cc/2L9K-4ZY2 (highlighting earlier research which proved Amazon's Rekognition technology to be deficient in recognizing darker-skinned faces when compared to its accuracy on lighter-skinned counterparts). Joy Buolamwini, a researcher for the MIT Media Lab who had done research of her own on the gender discrepancies in facial recognition, raised attention to the algorithmic bias associated with facial recognition prior to its acknowledgement as a more mainstream issue. *Id.* *See also* Shirin Ghaffary, *How to avoid a dystopian future of facial recognition in law enforcement*, VOX (Dec. 10, 2019), *archived at* https://perma.cc/4BUC-764S (noting that Buolamwini's widely-cited 2018 study, which "found that three leading facial recognition tools — from Microsoft, IBM, and Chinese firm Megvii, were incorrect as much as a third of the time in identifying the gender of darker skinned women, as compared to having only a 1 percent error rate for white males."). This finding helped pave the way for critics of algorithmic bias in facial recognition technologies. *Id.*

[12] *See* Hengtee Lim, *The Facial Recognition AI Timeline of 2020*, LIONBRIDGE (Oct. 12, 2020), *archived at* https://perma.cc/PKT3-HX4T (organizing the overall timeline of facial recognition's rise to common use, and the ultimate decision of several U.S. cities to ban law enforcement from using such technology); Harwell, *supra* note 10 (listing the local governments who have banned their police force from using the technology). *See, e.g.*, Boston, Mass., Ordinance No. 0683 (Jun. 24, 2020) (demonstrating an example of a city's ordinance banning the technology). *See* Shannon Flynn, *13 Cities Where Police Are Banned From Using Facial Recognition Tech*, INNOVATION & TECH TODAY (Nov. 18, 2020), *archived at* https://perma.cc/FRR5-CCLF (highlighting the list of cities, as of April 2021, which have banned the technology include Somerville, Cambridge, Brookline, Northampton, Springfield, and Boston, Massachusetts; Portland, Maine; Minneapolis, Minnesota; Portland, Oregon; Jackson, Mississippi; and San Francisco, Oakland, Alameda, and Berkeley, California). *See also* Denise Lavoie, *Virginia lawmakers ban police use of facial recognition*, ABC NEWS (Mar. 29, 2021), *archived at* https://perma.cc/3JFS-ELPQ (reporting how the state of Virginia passed a state-wide ban on law enforcement's use of the technology, effective July 1, 2021); Tyler Sonnemaker, *Portland becomes the first city to ban the use of facial*

Without federal legislation banning or extensively regulating facial recognition technology, the scope and scale of governmental application compounded with the technology's algorithm biases poses a potential for severe privacy violations and discriminatory practices.[13]

Facial recognition technology, in both the commercial and governmental spheres, has developed exponentially since its inception in the 1960s. This type of technology imposes grave concerns in the context of the Supreme Court's Fourth Amendment analysis of principles of privacy. Furthermore, there is a great risk of bias against minority groups through the application of this technology due to glaring lapses in the software's training data. The use of facial recognition technology endangers the privacy rights of citizens in

recognition technology by government agencies and private entities in public spaces, BUS. INSIDER (Sept. 10, 2020), *archived at* https://perma.cc/3E7A-LRT6 (reporting how Portland authorized a landmark ban on the use of facial recognition by prohibiting both government organizations and private companies and individuals from using it public spaces); Kate Conger et al., *San Francisco Bans Facial Recognition Technology*, THE N.Y. TIMES (May 14, 2019), *archived at* https://perma.cc/AUR7-S9W8 (detailing the first ban of its kind in the United States, prohibiting the police and other governmental agencies from using facial recognition software).

[13] *See* GARVIE ET AL., *supra* note 2, at 3 (postulating the negative repercussions of allowing mass surveillance without regard to the disparate treatment towards minority groups, as well as the privacy concerns that accompany unregulated police use of facial recognition); Maureen Ohlhausen, Cynthia Cole & Ryan Dowell, *Bias in Facial Recognition: Renewed Scrutiny of an Old Problem*, LAW.COM (July 8, 2020), *archived at* https://perma.cc/F9WD-L49K (highlighting the dangers of using software with algorithm biases that compromise accuracy); Shira Ovide, *A Case for Banning Facial Recognition*, THE N.Y. TIMES (June 9, 2020), *archived at* https://perma.cc/9QEM-UVF6 (highlighting how facial recognition systems' large disparities in error rates presents a palpable danger for those disproportionately affected and suggesting that the "combination of overreliance on technology, misuse and lack of transparency . . . is dangerous"); *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012) [hereinafter *What Facial Recognition Technology Means*] (statement of Sen. Al Franken, Chairman, Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary) (expressing how the potential helpfulness and power of facial recognition is countered by the threat of its abuse). Sen. Franken further warned against government collection of faceprints, acknowledging that "your face is a conduit to an incredible amount of information about you, and facial recognition technology can allow others to access all of that information from a distance, without your knowledge, and in about as much time as it takes to snap a photo." *What Facial Recognition Technology Means, supra*.

public spaces and poses harmful threats of mass surveillance, especially in consideration of the potential for discrimination and racial profiling. Law enforcement's widespread implementation of facial recognition systems poses major potential for invasive and abusive strategies of policing; therefore, strict prohibitive limitations and restrictions must be imposed on a federal level to solidify a national stance discouraging extreme surveillance measures.

II. History

A. Origins: Facial Recognition's Evolution and its Implementation by Governmental Entities

1. Developmental History

Starting in the 1960s, research on facial recognition technology began in the United States.[14] Government-funded private companies were tasked with conducting research in computer science, motivated largely by the desire for technological dominance in the midst of Cold War competition.[15] Early mechanisms for facial recognition improved

[14] *See* Carmen Aguado, *Facebook or Face Bank*, 32 LOY. L.A. ENT. L. REV. 187, 191 (Jan. 1, 2011) (chronicling the beginning stages of semi-automated facial recognition systems). The first types of facial recognition software required a system administrator to identify key features in a photograph. *Id.* Once this step was complete, the software could automatically calculate the distances between features and in doing so, compare the photograph to the reference. *Id.* *See also* KELLY A. GATES, OUR BIOMETRIC FUTURE: FACIAL RECOGNITION TECHNOLOGY AND THE CULTURE OF SURVEILLANCE 39–40 (2011) (explaining how the Department of Defense and intelligence agencies, in the 1960s, funded research labs to begin programming computers to identify human faces). Panoramic Research Inc., a private company based in Palo Alto, California, is one example of such a company created with the intention of conducting government-funded computer science research. *Id.* The projects were funded largely by the U.S. Department of Defense which entangled its functions in the Cold War goal of establishing "technological superiority." *Id.* While not all of the computer scientists were working to satisfy military-related projects, the fact that funding was tied to these priorities led to an emphasis on such needs. *Id.*

[15] *See id.* at 40 (describing the government's "post-Sputnik" rush to fund private companies in their biometric research). Although the programmers' research was not entirely directed to a military purpose, they experienced pressure to "emphasize the applicability of their work to Cold War priorities in order to secure funding from the Defense Advanced Research Projects Agency (DARPA) and its Information Processing Techniques Office (IPTO)." *Id.* at 40–41.

using a system for manual image matching developed by Woodrow Wilson Bledsoe, referred to as the "father of facial recognition."[16] Bledsoe's procedure involved the manual classification of photos through the use of a device called a RAND tablet, which was used to record the locations of facial features and add them to a database.[17] This system evolved over the next decade with researchers refining such manual recognition to include twenty-one specific facial markers.[18] In the late 1980s and early 1990s, further strides in facial recognition technology were made through development of the Eigenface approach, where feature analysis was conducted to create a set of basic identifying characteristics.[19] This crucial advancement heralded the automatic recognition and identification of one image in

[16] *See* GATES, *supra* note 14, at 41–42 (recognizing Bledsoe as a major pioneer in artificial intelligence research and detailing his development of a process called "feature extraction"). *See also The History of Face Recognition*, FACEFIRST (Aug. 1, 2017), *archived at* https://perma.cc/A69G-UNGR (acknowledging Bledsoe's work, although limited by the computing processing power of the time, was crucial to solidifying face recognition as a potential biometric).

[17] *See id.* (defining the RAND tablet and detailing the process of its use).

> Working in the 1960s, Bledsoe developed a system that could classify photos of faces by hand using what's known as a RAND tablet, a device that people could use to input horizontal and vertical coordinates on a grid using a stylus that emitted electromagnetic pulses. The system could be used to manually record the coordinate locations of various facial features including the eyes, nose, hairline and mouth. These metrics could then be inserted in a database. Then, when the system was given a new photograph of an individual, it was able to retrieve the image from the database that most closely resembled that individual.

Id.

[18] *See id.* (chronicling the next major development in facial recognition technology, which involved the use of subjective markers such as lip thickness and hair color); GATES, *supra* note 14, at 43 (citing the aim of the scientists, who worked at Bell Labs, was to design an algorithm that played off the strengths of both man and machine — specifically, to capitalize on the human adeptness in detecting facial features, and the machine's skillfulness in assessing statistics).

[19] *See The History of Face Recognition*, *supra* note 16 (explaining how Sirovich and Kirby built upon past research by using linear algebra to demonstrate how a set of blended features could be derived from performing feature analysis on various facial images). They were able to code a normalized face image using less than one hundred values. *Id.* *See also* Matthew Turk & Alex Pentland, *Eigenfaces for Recognition*, 3 J. OF COGNITIVE NEUROSCI. 71, 71–72 (1992) (differentiating their approach from previous research by emphasizing its advantage in "its speed and simplicity, learning capacity, and insensitivity to small or gradual changes in the face image").

relation to other images in a database, eliminating the need for a human system administrator to manually locate the facial features.[20] The 1990s represent a period of time dominated by a significant increase in research interest, largely attributable to a general increase in commercial projects, advancements in real-time hardware, and society's growing impetus for surveillance applications.[21] By the 2010s, exponential advancements in computing power and acquisition of large quantities of data for algorithm training allowed neural networks to become the new standard for facial recognition.[22]

2. Uses of Facial Recognition in Practical Application

Facial recognition technology is a general reference to the use of artificial intelligence to analyze biometrics of the face for purposes of identification or classification.[23] The science behind this technology relies on the development and training of an algorithm, the

[20] *See* Aguado, *supra* note 14 (capturing the novelty of Turk and Pentland's fully automated real-time method).

[21] *See* Rama Chellappa et al., *Human and Machine Recognition of Faces: A Survey*, 83 PROC. OF THE INST. OF ELECTRICAL AND ELECTRONICS ENGINEERS 705, 706 (1995) (outlining potential reasons why the research efforts toward facial recognition technology increased during the 1990s).

[22] *See* Tom Taulli, *Facial Recognition Bans: What Do They Mean For AI (Artificial Intelligence)?*, FORBES (June 13, 2020), *archived at* https://perma.cc/N58X-JZY2 (specifying the complexity of neural networks, which are sophisticated yet prone to gross misidentifications if there are discrepancies in the dataset on which the algorithm is based); GATES, *supra* note 14, at 62 (defining neural networks, otherwise referred to as "'connectionist' computational models," as simple units of processing organized in a larger network which "presumably simulate brain function by learning for themselves."). When the term "neural network" began being used in reference to a computer program, it "implied that computers could now do what the human brain could do, at the very least renewing the lofty promises of artificial intelligence . . ." GATES, *supra* note 14, at page 62.

[23] *See* ERIK LEARNED-MILLER ET AL., FACIAL RECOGNITION TECHNOLOGIES IN THE WILD: A CALL FOR A FEDERAL OFFICE 3 (May 29, 2020), *archived at* https://perma.cc/YC3C-4F5M (identifying "facial recognition technology" as "a catchall phrase to describe a set of technologies that process imaging data to perform a range of tasks on human faces, including detecting a face, identifying a unique individual, and estimating demographic attributes."). *See also* FEDERAL TRADE COMMISSION, BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES 1 n.2 (2012), *archived at* https://perma.cc/BTK4-T8ZR (articulating a broader definition of facial recognition would refer to "any technology that is used to extract data from facial images.").

creation of a template database for comparative purposes, and the process of comparing probe images to the database.[24] The algorithm is created with the purpose of detecting faces within an image and then examining the distance between individual features as a means of quantifying the data within the image.[25] The functional applications of facial recognition fall within one of two major categories: "one-to-one" and "one-to-many" matching.[26] The former, also referred to as facial verification, compares a target image to an image of the subject to confirm the subject's identity.[27] On the other hand, the latter seeks to identify an unknown subject by comparing one image to a large quantity of other images, seeking a match.[28]

Understanding the algorithmic mechanisms behind facial recognition technology provides insight as to how they are often prone to systemic errors.[29] Machine-learning algorithms "learn" facial

[24] *See* Barrett, *supra* note 7, at 230–31 (detailing the necessary elements in the process of conducting facial recognition analysis).

[25] *See id.* at 231 (providing an explanation of the algorithm's assessment process). Once the algorithm has detected a face, it seeks to calculate the distances between key features with the goal of numerically quantifying them in a template. *Id.*

[26] *See NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NIST (Dec. 19, 2019) [hereinafter *NIST Study*], *archived at* https://perma.cc/7Y2S-SRKV (describing the differences between "one-to-one" and "one-to-many" matching); Eifeh Strom, *Facing challenges in face recognition: one-to-one vs. one-to-many*, ASMAG.COM (Sept. 19, 2016), *archived at* https://perma.cc/6TFM-FB8K (comparing the relative advantages and disadvantages of one-to-one vs. one-to-many matching). One-to-one matching is easier to use and are often used in a controlled environment with optimal settings, making it easier to perform an identification. Strom, *supra*. Alternatively, most one-to-many systems must adapt to challenges such as "non-cooperative users, low/changing lighting conditions, and existing equipment/infrastructure." *Id.*

[27] *See NIST Study*, *supra* note 26 (defining one-to-one matching). "One-to-one" matching is often used for verification purposes, such as "unlocking a smartphone or checking a passport." *Id.*

[28] *See id.* (differentiating one-to-many matching from one-to-one matching). "One-to-many" matching describes the purpose of determining whether the person in a designated photo matches another photo in a database, and is a process often used to identify of a person of interest. *Id.*

[29] *See* Barrett, *supra* note 7, at 231 (conjecturing that the programming behind the algorithms is responsible for the discrepancies in output which lead to misidentifications). *See also NIST Study*, *supra* note 26 (weighing the gravity of different classes of error that measure an algorithm's performance). A false positive refers to a software's incorrect classification of photos of two different individuals as the same person. *Id.* A false negative is indicative of a software failing to identify a match between two photos of the same person. *Id.* This distinction is necessary

features by training on a dataset of images; therefore, the creators of these algorithms depend on a large and varied dataset for accuracy.[30] If a dataset is comprised of images from a majority demographic, the algorithm is unlikely to identify faces of minority groups with the same level of accuracy.[31] Therefore, the heterogeneity and the size of a database is crucial to ensuring the aptitude of the algorithm's performance.[32] Image quality also impacts algorithmic assessment—dark, low-resolution images, for example, are more difficult to analyze.[33] Additionally, both "one-to-one" and "one-to-many" searches can result in false positives or false negatives.[34] A "false

because the "class of error and the search type can carry vastly different consequences depending on the real-world application." *Id.*

[30] *See* Barrett, *supra* note 7, at 231–32 (explaining that algorithms are developed using training data and then subsequently tested using a "benchmark," therefore its accuracy is a direct reflection of the database from which it "learns"); Harwell, *supra* note 10 (recounting the results of the NIST study which proved that "most of the facial-recognition algorithms exhibit 'demographic differentials' that can worsen their accuracy based on a person's age, gender or race.").

[31] *See* Barrett, *supra* note 7, at 231 (reiterating an algorithm's dependence on training data for accurate performance). For example, an algorithm that is created through the process of "training on a dataset predominantly composed of images from one particular demographic, such as white men, will tend to perform less accurately for other groups whose faces do not resemble what the algorithm has been built to interpret as a 'face.'" *Id. See also Facial Recognition Technology (FRT): Hearing Before the H.R. Comm. on Homeland Sec.*, 116th Cong. 2–3 (2020) (testimony of Charles Romine, Director, Information Technology Laboratory) (elaborating on the necessary process of assessing "the core algorithmic capability of biometric recognition technologies and reported the accuracy, throughput, reliability, and sensitivity of algorithms with respect to data characteristics, for example, noise or compression, and to subject characteristics, for example, age or gender" in order to identify the lapses that may arise due to the use of training data that is not fully representative).

[32] *See* Barrett, *supra* note 7, at 231 (describing the use of a "benchmark" as a test to measure algorithmic accuracy: one that relies on a large and diverse dataset). Databases for benchmark purposes are used to create a "test intended to measure the accuracy of a facial recognition system as applied to a certain task or under certain circumstances." *Id.* at 231–32. If the photos supplying this database are homogeneous, the algorithm is bound to perform with less accuracy. *Id.* at 232.

[33] *See Face Recognition*, ELEC. FRONTIER FOUND. (Oct. 24, 2017), *archived at* https://perma.cc/6WJM-39YR (describing the increased potential for errors when the photo being analyzed is characterized by "poor lighting, low quality image resolution, and suboptimal angle of view").

[34] *See id.* (distinguishing facial recognition systems' rate of false negatives from that of false positives); KRISTIN FINKLEA ET AL., CONG. RSCH. SERV., R46586, FEDERAL LAW ENFORCEMENT USE OF FACIAL RECOGNITION TECHNOLOGY 9 (2020)

positive" describes the situation that occurs when the algorithm identifies a match, but does so erroneously.[35] Alternatively, a "false negative" refers to the face recognition system failing to match a face to another image that is, in fact, in the database being used.[36] Awareness as to the prevalence of these two types of errors is crucial to developers as they adjust their software for a particular purpose—the relative implication of a high rate of false positives versus a high rate of false negatives differs depending on the manner in which the technology is applied.[37]

Beginning with government funding of private research in the early stages of development, the respective roles of both state and private interests in facial recognition remain intricately entangled.[38] As facial recognition technology has evolved and become more accessible, an increasing number of private entities have begun to

[hereinafter FEDERAL LAW ENFORCEMENT USE OF FACIAL RECOGNITION TECHNOLOGY] (differentiating the two types of error and naming specific factors that may contribute to this error, such as "pose, illumination, and expression" in the case of false negatives).

[35] *See Face Recognition*, *supra* note 33 (exemplifying a false positive using the hypothetical where "a police officer submits an image of 'Joe,' but the system erroneously tells the officer that the photo is of 'Jack.'").

[36] *See id.* (explaining that in the case of a false negative, "the system will erroneously return zero results in response to a query").

[37] *See id.* (detailing the differing levels of significance that can result from a false negative or a false positive, depending on the situation).

> When researching a face recognition system, it is important to look closely at the "false positive" rate and the "false negative" rate, since there is almost always a trade-off. For example, if you are using face recognition to unlock your phone, it is better if the system fails to identify you a few times (false negative) than it is for the system to misidentify other people as you and lets those people unlock your phone (false positive). If the result of a misidentification is that an innocent person goes to jail (like a misidentification in a mugshot database), then the system should be designed to have as few false positives as possible.

Id.

[38] *See* GATES, *supra* note 14, at 63 (noting the reasons for a rise in demand for commercial applications). "As with other biometrics, business demand for more effective forms of network security, consumer tracking, and labor control provided a promising path to institutionalization for commercial facial recognition systems, especially as computing technology became better able to manage a growing volume of visual images." *Id.*

develop methods of application in a variety of new contexts.[39] Systems involving facial recognition are desirable to commercial enterprises for several reasons, notably for safety and security purposes, to provide user authentication as a means of access to platforms, accounts, and services, and for marketing and customer service needs.[40] Perhaps society's first major commercial introduction to facial recognition technology arose through the ubiquity of social media—in 2010, Facebook implemented a facial recognition tool which allowed users to easily "tag" friends in photos.[41] Each day, over 350 million photos are uploaded and tagged using this feature.[42]

[39] *See* FUTURE OF PRIVACY FORUM, PRIVACY PRINCIPLES FOR FACIAL RECOGNITION TECHNOLOGY IN COMMERCIAL APPLICATIONS 1 (Sept. 2018) [hereinafter PRIVACY PRINCIPLES FOR FACIAL RECOGNITION TECHNOLOGY], *archived at* https://perma.cc/7QRA-SFVL (recognizing the growing opportunities for commercial application of facial recognition); *What is Facial Recognition Used For?*, REC FACES (Nov. 6, 2020), *archived at* https://perma.cc/8R79-47T6 (listing common practical uses for the technology, such as public security, device security, identifying genetic disorders, preventing retail crime, authorizing legal alcohol purchases, mobile recreational apps, marketing, assisting the blind with accessibility, social media, and authorizing secure transactions).

[40] *See* PRIVACY PRINCIPLES FOR FACIAL RECOGNITION TECHNOLOGY, *supra* note 39, at 1 (listing key business functions that have the potential to be enriched through the use of facial recognition). These functions are enriched because facial recognition allows commercial enterprises to have access to photo databases that can improve their overall security, accessibility, and marketability, for instance. *Id.* *See also* U.S. GOV'T ACCOUNTABILITY OFF., GAO-20-522, FACIAL RECOGNITION TECHNOLOGY: PRIVACY AND ACCURACY ISSUES RELATED TO COMMERCIAL USES 11 (2020) (providing several common commercial applications of facial recognition technologies, such as ensuring secure access, maintaining general safety and security (such as monitoring crowds in large venues), identifying users for indexing (such as Facebook's tagging feature), marketing, authenticating payments, and tracking or monitoring attendance).

[41] *See The History of Face Recognition*, *supra* note 16 (noting Facebook's early implementation of facial recognition into its social media business model). *See also Facebook settles facial recognition dispute*, BBC NEWS (Jan. 30, 2020), *archived at* https://perma.cc/2R6C-3QJR (reporting that Facebook's automatic tagging system was one of the first well-known commercial implementations of facial recognition; it was met with controversy as it did not require a user's consent to perform, although there was an option to de-activate the feature). The tagging feature was adapted in 2017 to allow users to toggle it on or off with more ease, and in 2019, as part of the company's privacy initiative, Facebook modified it once again to make users' consent mandatory before activation of the setting. *Id.*

[42] *See The History of Face Recognition*, *supra* note 16 (emphasizing the popularity of Facebook's "tagging" feature since its implementation in 2010); Russell Brandom, *Facebook is the only thing standing between us and a face-reading*

Beyond social media, other enterprises have been creatively deploying facial recognition in their business models; MasterCard, for instance, launched a feature called "selfie pay" in 2016, which allows users to authorize payments using facial authentication.[43] Shopping malls, drugstores, and grocery stores have begun implementing facial recognition software that evaluates emotional expressions in conjunction with real-time surveillance systems as a means of predicting or identifying shoplifters.[44] In an effort to identify high-paying customers, entertainment establishments such as casinos, restaurants, and hotels are also making use of this emotion-sensing technology.[45]

However, inhibited by concerns surrounding consent and potential liability, private uses of facial recognition technology have

nightmare app, THE VERGE (Mar. 15, 2017), *archived at* https://perma.cc/WMB3-K9WY (noting that the statistic of 350 million photos per day indicates that Facebook is well on its way to having one trillion photos on its website). *See also Nothing personal? How private companies are using facial recognition tech*, TECHHQ (June 8, 2020) [hereinafter *Nothing personal?*], *archived at* https://perma.cc/EY7Y-M9AY (noting that major facial recognition services, such as Clearview AI, have been criticized for "scrapping" images from Facebook's extensive photo databases).

[43] *See id.* (providing examples of facial recognition technology in the mainstream corporate landscape). For example, cosmetic companies, such as MAC, are using in-store augmented reality mirrors to allow customers to virtually experiment with products. *Id.* Other companies, namely Walmart and McDonald's, have experimented with mood-sensing technologies to analyze the emotional states of customers and employees. *Id. See also* Natasha Lomas, *MasterCard launches its 'selfie pay' biometric authentication app in Europe*, TECHCRUNCH (Oct. 4, 2016), *archived at* https://perma.cc/NT78-5XAM (detailing the rollout of MasterCard's new feature). MasterCard has cited convenience and lowering the risk of fraud as two main catalysts behind their decision to roll out the new feature. *Id.* Following in Apple's footsteps after their introduction of similarly convenient Apple Pay, MasterCard is "seeking to grease the wheel of ecommerce." *Id.*

[44] *See* Barrett, *supra* note 7, at 233 (listing various commercial applications of the software). These uses manifest in a wide array of commercial sectors. *Id.* These uses include customer identification and security purposes to prevent shoplifting in retail environments; identifying persons of interest or high-paying customers in entertainment and hospitality industries; and verifying patients in hospitals as well as passengers on airlines. *Id.* at 233–35. Facial recognition has also been deployed alongside emotional-inference technologies to anticipate disposition in schools and other relevant contexts. *Id.* at 235.

[45] See *id.* at 233–35 (describing more uses in the private sector). Further, many of these commercial uses are not disclosed to a base of consumers, and their ubiquity makes it almost impossible for patrons to opt out of inclusion. *Id.*

proven more ideal in theory than in practice.[46] Legal precedent involving suits brought against Facebook for violating the 2008 Illinois Biometric Privacy Act resulted in disagreement among different judicial circuits, thus opening the floodgates to similar class-action suits.[47] In June 2020, two Illinois residents sued Amazon, Google, and Microsoft for violating the same statute, which forbids the collection, storage, and use of biometric information without affirmative consent.[48] The issue of obtaining consent, coupled with external pressure in light of emerging research exploring algorithms' technical flaws and biases, created a large obstacle for many manufacturers of facial recognition software—Microsoft, Amazon,

[46] *See* Mark MacCarthy, *Who thought it was a good idea to have facial recognition software*?, BROOKINGS (Aug. 20, 2020), *archived at* https://perma.cc/D3PB-HQGJ (explaining how "combining consent with a private right of action creates conflicts to obtain the former"). Allowing for a private right to action has previously led to costly litigation, as there exists a potential that billions of people could prove injury and be therefore entitled to compensation. *Id.*

[47] *See* Patel v. Facebook, Inc., 932 F.3d 1264, 1267 (2019) (affirming that Facebook violated concrete privacy interests of Facebook users under Illinois's Biometric Information Privacy Act). *See also* MacCarthy, *supra* note 46 (detailing how, in February 2020, Facebook settled the lawsuit for $550 million). *See also* Kashmir Hill, *Your Face is Not Your Own*, THE N.Y. TIMES (Mar. 18, 2021), *archived at* https://perma.cc/ZK3X-GATG (explaining how Illinois's Biometric Information Privacy Act (BIPA) is a major legal obstacle for facial recognition services (namely Clearview AI), because it requires that "private entities must receive individuals' consent to use their biometrics . . . or incur fines of up to $5,000 per use"). This statute, which has empowered the American Civil Liberties Union (ACLU) and approximately ten other alleged victims to file suit, has forced Clearview to remove from its database any photos sourced from Illinois, looking to photos' embedded geographical information. *Id.*

[48] *See* Steven Musil, *Amazon, Google, Microsoft sued over photos in facial recognition database*, CNET (July 14, 2020), *archived at* https://perma.cc/99KW-SY4S (detailing the allegations of Illinois residents Steven Vance and Tim Janecyk in their federal lawsuit against the corporations). The two plaintiffs say that the companies blatantly violated the Illinois law by including their images in a data set without the owners' consent, despite the fact that they were both clearly identifying themselves as Illinois residents and therefore protected by the BIPA statute. *Id.* For example, Janecyk and Vance's suit alleges that the defendants "chose to use and profit from biometric identifiers and information scanned from photographs that were uploaded from Illinois; managed via Illinois-based user accounts, computers and mobile devices, and/or created in Illinois," therefore knowingly exposing Illinois residents to privacy risks. *Id.*

and IBM, for example, have all recently decided to halt or abandon the distribution of their technology to law enforcement agencies.[49]

Law enforcement has co-opted facial recognition technology since its early stages.[50] In 1988, when the technology was still only semi-automated, the Lakewood Division of the Los Angeles County Sheriff's Department analyzed the faces of suspects from surveillance tape video evidence by comparing it to its database of mugshots.[51] In 1994, the Immigration and Naturalization Service developed the Automated Biometric Identification System ("IDENT") as an instrument for use by the United States Border Protection, which contained 1.8 million biometric identities within five years of operation.[52] Following the September 11, 2001 terrorist attacks, the U.S. government instituted widespread security measures through the

[49] *See* Karen Hao, *The two-year fight to stop Amazon from selling face recognition to the police*, MIT TECH. REV. (June 12, 2020), *archived at* https://perma.cc/DCY9-3AJY (detailing Amazon's announcement of a one-year moratorium on police use of its software, Rekognition, IBM's discontinuation of its facial recognition system, and Microsoft's decision to halt sales of its system to law enforcement until the technology is regulated by federal law); *see also* Woodrow Hartzog, *Facial Recognition is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), *archived at* https://perma.cc/B2FM-KH9L (expressing how the ACLU and almost 70 other civil rights organizations asked Amazon to stop selling their software to law enforcement agencies). *See generally* Ari Levy & Lauren Hirsch, *Amazon bans police use of facial recognition technology for one year*, CNBC (June 10, 2020), *archived at* https://perma.cc/6658-AJ9M (reporting on Amazon's moratorium).

[50] *See Biometrics in History*, DEPARTMENT OF HOMELAND SEC. (July 13, 2020) [hereinafter Biometrics History], *archived at* https://perma.cc/726K-3C3G (detailing the history of government use of biometric identifiers). *See also* FEDERAL LAW ENFORCEMENT USE OF FACIAL RECOGNITION TECHNOLOGY, *supra* note 34, at 1 (describing how "law enforcement agencies' use of facial recognition technology (FRT), while not a new practice, has received increased attention from policymakers and the public"). The report further explains some of the many purposes for which federal, state, and local law enforcement have used facial recognition over the years, specifically noting that "the Federal Bureau of Investigation (FBI) uses the technology to aid its investigations, and the bureau provides facial recognition assistance to federal, state, local, and tribal law enforcement partners" while state and local law enforcement agencies apply the same to their investigations, as well as border officials. *Id.*

[51] *See* Aguado, *supra* note 14, at 192 (describing how Los Angeles Country Sherriff's Department's Lakewood Division used a semi-automated facial recognition system in 1988).

[52] *See* Biometrics History, *supra* note 50 (describing how facial recognition was implemented for the purpose of border security).

use of biometric identification.[53] Private companies soon received funding for research and technological development with the goal of implementing such biometric systems into domestic safety objectives.[54] With the technology constantly evolving, federal, state, and local police departments nationwide have implemented facial recognition software for a variety of purposes, such as generalized surveillance, targeted tracking, or as a means of identification.[55] Over 117 million American adults are now included in a law enforcement face recognition network, and at least 26 states permit running searches against their databases of driver's license photos.[56]

[53] *See* Kelly Gates, *IDENTIFYING THE 9/11 'FACES OF TERROR'*, 20 CULTURAL STUDIES 417, 417 (2006) [hereinafter *FACES OF TERROR*] (explaining the growing concern toward the implementation of security measures following the attacks on September 11th); Aguado, *supra* note 14, at 192 (describing how 9/11 served as an impetus for the government's use of biometric identifiers). *See also* Ritchie S. King, *How 5 Securities Fared After 9/11*, IEEE SPECTRUM (Aug. 31, 2011), *archived at* https://perma.cc/RN9V-HELS (representing that facial recognition engineers "made a 20-fold improvement in accuracy between 2000 and 2006").

[54] *See FACES OF TERROR*, *supra* note 53, at 417 (describing the government's objective to invest in biometric research as a means of identification for security purposes). *See also* King, *supra* note 53 (explaining how 9/11 "sparked a security mania in the United States that included a brassbound push for new surveillance technology"). This push for domestic security included efforts such as imaging software used for airline passengers, radiation detectors for cargo imports, and explosive-trace detectors. *Id.*

[55] *See* Barrett, *supra* note 7, at 236 (listing some of the various governmental uses of facial recognition technology); FEDERAL LAW ENFORCEMENT USE OF FACIAL RECOGNITION TECHNOLOGY, *supra* note 34, at 4 (highlighting specific instances in which law enforcement can use facial recognition, including for the purposes of "generating investigative leads, identifying victims of crimes, facilitating the examination of forensic evidence, and helping verify the identity of individuals being released from prison"). The report further elaborates that "the frequency and extent to which FRT is used at various phases of the criminal justice system (from generating leads and helping establish probable cause for an arrest or indictment, to serving as evidence in courtrooms) is unknown." *Id.* at 5. *See generally* Mark Harris, *How Facial Recognition Technology Is Helping Identify the U.S. Capitol Attackers*, IEEE SPECTRUM (Jan. 11, 2021), *archived at* https://perma.cc/E8YB-ZZ2X (describing how facial recognition was used to identify those who flooded the U.S. Capitol on January 6, 2021).

[56] *See* GARVIE ET AL. *supra* note 2, at 2 (emphasizing that "face recognition is neither new nor rare"). FBI-run facial recognition searches are more commonly conducted than federal wiretaps. *Id.* Approximately one-in-four state or local police departments has access to other agencies' databases and systems for face recognition searches, and potentially 30 states allow law enforcement to conduct searches against

B. *Unpacking the Evolutionary Judicial History of Technology, Privacy, and the Fourth Amendment*

While the Supreme Court has not specifically addressed the constitutional limits of facial recognition technology, its approach to digital technologies is relevant in determining the limits of the government's power when juxtaposed with individual privacy rights.[57] The Supreme Court has previously applied the spirit of the Fourth Amendment to digital technologies but has recognized limitations in doing so.[58] In 1967, the Supreme Court, in *Katz v. United States*, extended Fourth Amendment protection against unreasonable searches and seizures to apply to electronic wiretaps of telephone conversations, establishing that searches do not necessarily need to involve a physical manipulation of a person's property.[59] The Court's two-pronged

databases of driver's license and ID photos. *Id.* About half of all Americans have been subjected to such a search. *Id.*

[57] *See* Hirose, *supra* note 1, at 1595 (explaining how there is a lack of legislature and jurisprudence regarding the limitations of facial recognition technology); KELSEY Y. SANTAMARIA, CONG. RSCH. SERV., R46541, FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT: SELECT CONSTITUTIONAL CONSIDERATIONS 3 (2020) [hereinafter FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT] (presenting the fact that "[t]o date, there is no federal framework specifically directed at the use of FRT by government and private entities"). Despite this lack of unifying federal legislation, there is a patchwork of generally applicable legislation addressing certain elements of biometric screening that may be relevant to facial recognition. *Id.*

[58] *See* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1, 5–6 (forthcoming 2021) (emphasizing the challenge in applying the protections delineated by the U.S. Constitution to contemporary society).

[59] *See* Katz v. United States, 389 U.S. 347, 348–51 (1967) (holding that individuals maintain a reasonable expectation of privacy when using a phone booth). This marks a transition in analysis from a previous emphasis on principles of property law to one that relies upon notions of privacy. *Id.* at 350–51. While the Fourth Amendment protects the sanctity of the home and other physical property, *Katz* and other subsequent decisions broadened Fourth Amendment protections. *Id.* at 351. "The Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id. See also* United States v. Karo, 468 U.S. 705, 715 (1984) (holding that police officers violate an individual's reasonable expectation of privacy when monitoring a GPS "beeper" in a private residence); Kyllo v. United States, 533 U.S. 27, 34 (2001) (holding that use of

analysis established that there must first be a subjective expectation of privacy, and second, that society recognize that expectation as reasonable.[60] Since then, in several instances, the Supreme Court has determined digital information to be within the purview of the Fourth Amendment.[61] In *United States v. Jones,* the Supreme Court's majority opinion established that placement of a GPS tracking device on a suspect's car constituted a "trespass," and therefore qualified as a search under the Fourth Amendment.[62] The concurring opinion, written by Justice Sotomayor, particularly stresses the dangers of government access to personal information, emphasizing that "the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[63] Later, in *Riley v. California,* the Supreme Court precluded warrantless searches of cell phones seized during an arrest, acknowledging the privacy interest in personal digital data.[64] Finally, in *Carpenter v. United States*, the

thermal sensors to monitor a home violates an individual's reasonable expectation of privacy).

[60] *See Katz,* 389 U.S. at 361 (Harlan, J., concurring) (setting forth a two-pronged analysis for determining whether a person has a privacy interest). "There is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.*

[61] *See* Ferguson, *supra* note 58, at 25 (marking several post-*Katz* Supreme Court decisions that applied privacy evaluations to include digital mechanisms, representing a sense of flexibility in Constitutional analysis).

[62] *See* United States v. Jones, 565 U.S. 400, 400 (2012) (recognizing that the government's 28-day tracking of a suspect's car using a GPS device constituted trespass). The Court addressed *Katz v. United States* by clarifying that the Fourth Amendment is supplemented by trespass under property law. *Id.* at 409. Its analysis stated that the governments' physical act of attaching a GPS tracker violated the Fourth Amendment under *Katz*. *Id.* at 400.

[63] *See id.* at 415 (Sotomayor, J., concurring) (warning against allowing governmental access to data that captures the most intimate details of individuals' personal lives).

[64] *See* Riley v. California, 573 U.S. 373, 401 (2014) (precluding warrantless searches of cell phones seized during an arrest). The Supreme Court's holding does not immunize cell phone information from searches, but instead requires that such searches are done with a warrant even when the search is a result of a seizure incident to arrest. *Id.* Prior to *Riley*, whether a warrant was required to search digital data was jurisdictionally split. *Id.* *See also* Patrick E. Corbett, *The Fourth Amendment and Cell Site Location Information: What Should We Do While We Wait for the Supremes*, 8 FED. CTS. L. REV. 215, 215 (2015) (emphasizing *Riley*'s significance in the interpretation of the Fourth Amendment). The Court's decision in *Riley* represented its willingness to address more difficult applications of the Fourth Amendment. *Id.*

Supreme Court held that an individual maintains a legitimate expectation of privacy in the historical record of his or her physical movements as captured through cell site location information ("CSLI").[65] In *Carpenter*, the government's access of 127 days of CSLI from a service provider invaded the defendant's reasonable expectation of privacy and therefore constituted a search.[66] Thus, the Court maintained that the government is generally required to obtain a search warrant supported by probable cause in order to access CSLI.[67]

III. Facts

The scope and scale of the commercial and governmental implementation of facial recognition technology became increasingly prevalent in recent years—a trend that appears to be directly proportional to the amount of controversy surrounding its use.[68]

[65] *See* Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (holding that an individual maintains a legitimate expectation of privacy in historical CSLI, opening the door to the protection of other forms of digital data). *See also* Clare Garvie & Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, GEO. L. CTR. ON PRIVACY & TECH. (May 16, 2019), *archived at* https://perma.cc/XSF9-VYWF (summarizing how the court's decision in *Carpenter* can be applied to facial recognition).

[66] *See Carpenter*, 138 S. Ct. at 2216–19 (describing the factors that the Court considers in determining the existence of a reasonable expectation of privacy). The majority opinion references two separate lines of cases which intersected in *Carpenter*, the first being the inquiry as to "a person's expectation of privacy in his physical location and movements" and the second being whether an individual maintains a reasonable expectation of privacy in information shared with third parties. *Id.* at 2215–16.

[67] *See id.* at 2211 (holding that CSLI is protected under the Fourth Amendment). The Court held that the unique qualities of cell phone location information insulate it from being subject to the "third party doctrine," which typically allows the Government to access any information shared with a third party, per the logic that there is no reasonable expectation of privacy if the information is not kept private. *Id.* at 2216. *Carpenter* solidified that "whether the Government employs its own surveillance technology as in Jones or leverages the technology of a wireless carrier . . . an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." *Id.* at 2217.

[68] *See* Lane Brown, *There Will Be No Turning Back on Facial Recognition*, INTELLIGENCER (Nov. 2, 2019), *archived at* https://perma.cc/G7EH-JD8X (describing the recent pushback as "Face Panic" and calling the general feelings toward surveillance as one of "full-grown modern worry"); Nicole Martin, *The Major Concerns Around Facial Recognition Technology*, FORBES (Sept. 25, 2019), *archived at* https://perma.cc/L6JF-GPRZ (listing the concerns citizens have voiced

Recently, a release of data regarding facial recognition's widespread usage and unreliability catalyzed a shift of the general public's disposition towards the use of such technology.[69] What was once generally regarded as an effective tool has taken on a new reputation as an inescapably ubiquitous technology with a vast potential for misuse.[70]

A. A Tool or a Terror? The Scope and Scale of Governmental Application of Facial Recognition Technology

Facial recognition systems are neither new nor uncommon for law enforcement agencies.[71] According to Georgetown Law's 2016

regarding facial recognition, despite its expanding popularity in recent years and the increasingly large market for its use). Specifically referenced are the lack of federal regulations, the fear of wrongful convictions when used in criminal investigations, and its general invasiveness. Martin, *supra*.

[69] *See* Brown, *supra* note 68 (outlining the several events that occurred during 2019 which raised concerns about the widespread and growing use of facial recognition). Among the events listed are: the NYPD's use of facial recognition in conjunction with surveillance footage to arrest a man named Larry Griffin for planting a false bomb on a subway platform; the reports released in spring 2019 claiming that the FBI had access to hundreds of millions of images; the first local bans on law enforcement use springing up in U.S. cities; fears relating to a false rumor that a popular photo app was a smokescreen for the Russian government collecting users' faces; and research released indicating the presence of extreme algorithm bias. *Id.*

[70] *See* Rachel Metz, *Portland passes broadest facial recognition ban in the US*, CNN BUS. (Sept. 9, 2020), *archived at* https://perma.cc/A77D-KQ6J (providing the context for changing attitudes toward advancements in surveillance technology). While many of the benefits of the technology were previously embraced, many citizens have become increasingly uncomfortable with the idea of widespread facial recognition, especially in light of the recent studies proving the potential for racial bias or government misuse in conjunction with the lack of a unifying regulatory scheme. *Id.*

[71] *See* GARVIE ET AL., *supra* note 2, at 2 (stating that government use is common and widespread); Natasha Singer & Cade Metz, *Many Facial-Recognition Systems Are Biased, Says U.S. Study*, THE N.Y. TIMES (Dec. 19, 2019), *archived at* https://perma.cc/3PHE-TL7P (considering that "although the use of facial recognition by law enforcement is not new, new uses are proliferating with little independent oversight . . . ."). Furthermore, recent global uses have been met with increasing controversy, such as China's use of the technology to "surveil and control ethnic minority groups like the Uighurs." Singer & Metz, *supra*. Another example met with controversy was the United States Immigration and Customs Enforcement's use of the technology to surreptitiously analyze millions of peoples' drivers' licenses. *Id.*

study, police forces in the United States include over 117 million people in their facial recognition networks—a figure that equates to about half of all American adults.[72] Furthermore, the Federal Bureau of Investigation ("FBI") has actively used this type of technology since 2011 to assist its own investigations as well as that of state and local police.[73] Specifically, the FBI's Next Generation Identification ("NGI") database supplies state and local police forces with unregulated access to over 30 million records.[74] The FBI also has a unit, known as Facial Analysis, Comparison, and Evaluation Services ("FACE"), which is entirely dedicated to conducting searches—it can access over 400 million non-criminal photos, courtesy of records provided by state government agencies, namely departments of motor vehicles.[75] In the spring of 2019, the U.S. Government Accountability Office released information that the FBI has access to over 641 million photos of faces in a searchable database.[76] Even local databases tend

[72] *See* GARVIE ET AL., *supra* note 2, at 28 (specifying a figure that demonstrates governmental agencies' frequent use); Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where it Falls Short*, THE N.Y. TIMES (Jan. 12, 2020), *archived at* https://perma.cc/L6FR-Y8E7 (explaining the proportion of American adults included in a database).

[73] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-267, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY 15 (2016) (recognizing how the FBI has historically used facial recognition in its investigations).

[74] *See Face Recognition*, *supra* note 33 (acknowledging the unfettered access to information afforded to the FBI through the Next Generation Identification database of records). *See* FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT, *supra* note 57, at 5–6 (reporting that the FBI's NGI system includes a breadth of biometric identifiers, including fingerprints and iris scans, and has a separate component called the Interstate Photo System (IPS), which allows law enforcement agencies to search a database of photos with facial recognition software enabled). Similar systems used by the Department of Homeland Security (namely, IDENT) exist for purposes of monitoring U.S. borders. *Id.* at 6.

[75] *See Face Recognition*, *supra* note 33 (identifying the branch of the FBI which is specifically dedicated to facial recognition tasks and reporting the sources of photographs used as a database). FACE allows the FBI access to non-criminal photos from state DMVs and the State Department. *Id.* Presently, 16 states allow FACE to access photos from driver's licenses and IDs. *Id.*

[76] *See* Eli Watkins, *Watchdog says FBI has access to more than 641 million 'face photos'*, CNN (June 14, 2019), *archived at* https://perma.cc/Y4KA-2SGK (reporting the massive figure, 641 million face photos, as released by the U.S. Government Accountability Office in April 2019).

to be large.[77] Pinellas County Sheriff's Office in Florida, for example, has one of the most extensive databases, reportedly used by over 240 different agencies to make searches approximately 8,000 times a month.[78]

Facial recognition technology has multiple different practical applications for identification.[79] One of the most common practices, known as field identification, is the use of recognition software in the context of an encounter where a person fails to self-identify.[80] In this scenario, an officer will take a photo of the person and can attain an almost instant match to a database of mugshots, driver's license

[77] *See Face Recognition*, *supra* note 33 (noting the breadth of information afforded to the government, even in smaller municipalities); Valentino-DeVries, *supra* note 72 (specifying that the Pinellas County, Florida statewide program is one of the largest local government databases).

[78] *See Face Recognition*, *supra* note 33 (stating that "[d]atabases are also found at the local level, and these databases can be very large."). The Pinellas County database is almost fifteen years old and is potentially the country's most frequently used database. *Id.* *See also* GARVIE ET AL., *supra* note 2, at 4 (explaining that the Pinellas County system is "almost 15 years old and may be the most frequently used system in the country"). Its sheriff, when asked if the office audits for misuse, replied, "not really." *Id.*

[79] *See id.* at 10 (outlining the most popular practical applications of facial recognition software in everyday practices of law enforcement). Most of these uses fall into the categories of face verification, confirming a person's alleged identity, and face identification, which seek to identify a face that is unknown. *Id.* *See also* FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT, *supra* note 57, at 5 (explaining the specific manner in which law enforcement is likely to use facial recognition technologies as an identification tool). For instance, upon a person's arrest, "police may employ FRT and associated databases to compare the arrestee's mugshot with other images to determine the person's identity and criminal history" or may alternatively use it for identification in a noncustodial context. *Id.* Other uses include using a facial recognition system to identify faces from security camera footage for comparison with an existing suspect list, for monitoring travelers coming in and out of the U.S., or preventing duplicate issuance of government documentation, like driver's licenses or passports. *Id.*

[80] *See* GARVIE ET AL., *supra* note 2, at 11 (describing one of the most common uses of facial recognition, where police officers will use a smartphone or a tablet to take a picture of a person who fails to self-identify, and then uses that picture to search within a large database of photos); FACIAL RECOGNITION: FACING THE FUTURE OF SURVEILLANCE, PROJECT ON GOVERNMENT OVERSIGHT (2019) [hereinafter FACING THE FUTURE OF SURVEILLANCE] (elaborating on the common practice of field identification, in which facial recognition is used by police officers to identify someone they have encountered in the field, which "could include discussions with a witness or victim of a crime, but is likely to primarily focus on identifying individuals that an officer stops during a patrol").

photos, or other images.[81] This same process often occurs in the event of an arrest.[82] Similarly, during the course of a criminal investigation, it is not uncommon for police forces to seek a photo of a suspect, typically from social media or security camera footage, for the purpose of searching against their database of faces.[83] Furthermore, police forces often use facial recognition programs in conjunction with real-time video surveillance, which identifies a match when a specific face is identified on the live feed from a security camera.[84]

While police forces place a high value on this technology and acknowledge the usefulness of such a tool in conducting investigations, most agencies avoid disclosing their techniques to the general public.[85] For instance, the New York Police Department has

[81] *See* GARVIE ET AL., *supra* note 2, at 117 (further clarifying the process that ensues when an officer uses facial recognition for field identification).

[82] *See id.* at 118 (acknowledging that a similar process occurs when a person is arrested and taken into custody); FACING THE FUTURE OF SURVEILLANCE, *supra* note 80 (clarifying that in an arrest identification, an officer will use a mugshot photo to later find or confirm the arrested person's identity).

[83] *See* GARVIE ET AL., *supra* note 2, at 117 (describing the tendency for law enforcement agents to rely on facial recognition as a means of investigation into a subject's identity). *See* FACING THE FUTURE OF SURVEILLANCE, *supra* note 80 (describing the typical course of events when police use FRT for an investigative identification, a process which involves obtaining a photo of an unidentified suspect from video footage or another image source). The source of the image may manifest in the form of "crime scene footage, or police covertly photographing an unidentified suspect they are actively watching." *Id.* Subsequently, law enforcement has the ability to use facial recognition to find the suspect's identity and proceed. *Id.*

[84] *See* GARVIE ET AL., *supra* note 2, at 12 (noting that law enforcement will also use advanced facial recognition in conjunction with closed circuit TV footage, which allows officers to identify suspects either in a live broadcast or in archival footage); FACING THE FUTURE OF SURVEILLANCE, *supra* note 80 (explaining this tactic as a process of scanning all faces that appear on screen during a video feed and then comparing the collection of faces to a watchlist to identify specific individuals).

[85] *See* Schuppe, *supra* note 3 (confirming that many agencies keep their methods of surveillance secret as a means of protecting the integrity of investigation). *See* GARVIE ET AL., *supra* note 2, at 10 (referencing Professor Laura Donohue's scholarship which differentiates between older and newer systems of biometric identification, the latter of which is usually conducted much more secretively). Her research indicates that prior to the 21st century, governments used biometrics for specific identification, yet the process was usually transparent to the person, as it often required their cooperation—Donohue calls this Immediate Biometric Identification, or IBI. *Id.* On the other hand, today's advanced facial recognition fosters a more continual process of identification, referred to by Donohue as Remote Biometric Identification, or RBI, which allows law enforcement to do so remotely and therefore can be done secretly. *Id.*

repeatedly resisted efforts by critics and defense attorneys to learn more about the procedures used in their facial recognition identification.[86] Furthermore, the government's use of biometric databases is not only surreptitious in nature, but is also largely unregulated—very few laws delineate the extent to which law enforcement can utilize this information.[87]

B. Confronting the Presence of Algorithmic Biases

The accuracy of facial recognition technologies, like all artificial intelligence systems, is limited by the size and variety of the data from which it learns.[88] The National Institute of Standards and Technology ("NIST") published a study in December 2019 which applied a Face Recognition Vendor Test Program to assess 189 software algorithms created by 99 different developers.[89] The test evaluated the programs on how well they each perform both "one-to-one" and "one-to-many" matching by calculating the rate of false positives and false negatives produced.[90] The algorithms were tested using 18.27 million images of 8.49 million different people; each

[86] *See* Schuppe, *supra* note 3 (exemplifying this surreptitious use of the technology by noting how in "New York, the police department has resisted attempts by defense attorneys and privacy advocates to reveal how its facial recognition system operates.").

[87] *See id.* (noting the lack of boundaries set for law enforcement in using such a powerful tool).

> While some agencies have policies on how facial recognition is used, there are few laws or regulations governing what databases the systems can tap into, who is included in those databases, the circumstances in which police can scan people's photos, how accurate the systems are, and how much the government should share with the public about its use of the technology.

Id.

[88] *See NIST Study*, *supra* note 26 (explaining that error rates are related to the way an algorithm has "learned," therefore, characteristics of training data are indicative of an algorithm's performance).

[89] *See id.* (explaining how the study was conducted on a majority of the industry, and its purpose was to test the face recognition algorithms voluntarily submitted to NIST by a variety of developers by evaluating the algorithms' ability to execute different tasks).

[90] *See id.* (generally delineating the two types of tasks on which the algorithm is tested). The test is separated into two major tasks; the "one-to-one" task involves confirming that the person in one photo matches the same person in another photo, and the "one-to-many" task requires the software to see if the person in one photo has any matches in any other photo in the database. *Id.*

image also contained metadata indicating the subject's age, sex, and origin.[91] The study provided empirical evidence that most algorithms exhibit demographic differentials, which means that the accuracy rate of a match differs between demographic groups.[92] The study assessed each algorithm individually, but the results showed a general trend of lower accuracy rates for minority groups.[93] In the "one-to-one" matching tests, the algorithms demonstrated a higher rate of false positives for African American faces and Asian faces than those of Caucasians.[94] In certain cases, the error rate was 100 times higher.[95] Some of the algorithms developed in Asian countries, however, proved an exception to this trend—in these algorithms, no such disparity in the rate of error between Asian and Caucasian subjects existed, likely due to the fact that such developers used more diverse data sets to train these algorithms.[96] In terms of "one-to-many" matching, there was a significantly higher rate of false positives for African American females in particular.[97] False positives, NIST reports, are of particular

[91] *See id.* (noting the size and characteristics of the dataset used in the study). These images were sourced from four collections of photographs in databases provided by the State Department, the Department of Homeland Security, and the FBI. *Id.* None of the images used were "scraped" from internet databases such as those from social media sites. *NIST Study*, *supra* note 26.

[92] *See id.* (reporting the main results of the study, which confirmed that a majority of software, which represents most of the industry, demonstrate differential error rates for various demographics). For example, in the one-to-many matching task, the study reported higher rates of false positives for African American women. *Id.*

[93] *See id.* (describing how the algorithms perform worse in identifying certain groups of people). There were great discrepancies in the differentials for rates of error for different demographic groups. *Id.*

[94] *See id.* (explaining that false positives were a more common error in the case of members of minority groups than in that of Caucasians). The differentials between the rates of false positives for Caucasians versus Asians and African Americans often ranged from a factor of 10 to 100 times. *NIST Study*, *supra* note 26.

[95] *See* Harwell, *supra* note 10 (reporting researcher Joy Buolamwini's reaction to the differential of up to 100, which she describes as "a sobering reminder that facial recognition technology has consequential technical limitations alongside posing threats to civil rights and liberties.").

[96] *See NIST Study*, *supra* note 26 (noting that there were higher accuracy rates for some of the software developed in Asia).

[97] *See id.* (describing yet another instance of higher error rates when algorithms attempted to identify members of a minority group).

importance because the false identification of an innocent person is a pitfall society abhors.[98]

The NIST study identifies empirical evidence of differential error rates, but does not provide an explanation for why these variations occur.[99] Researchers have suggested that some demographics may be more difficult to identify than others.[100] For example, they have hypothesized that women, who are more likely to wear cosmetics, may be more difficult to recognize.[101] Other experts have reported that facial recognition is inherently reliant on color contrasts in images, which make the systems less adept at identifying

[98] *See NIST Study Finds Extensive Bias in Face Surveillance Technology*, ELEC. PRIV. INFO. CTR. (Dec. 20, 2019), *archived at* https://perma.cc/2G6F-FSFV (referencing the danger in an excess of false positives, which in a law enforcement context could lead to the improper arrests and convictions of innocent people); *see also* FEDERAL LAW ENFORCEMENT USE OF FACIAL RECOGNITION TECHNOLOGY, *supra* note 34, at 10 (noting the grave implications of false positives, which could potentially cause invalid investigations and false accusations).

[99] *See NIST Study*, *supra* note 26 (indicating that the statistical study does not provide information on the cause and effect of the algorithm's lapses). Although this difference in accuracy suggests that the developers in Asian countries used more diverse training data, the NIST study indicates that they are solely reporting the results of the tests and do not attempt to identify a cause-and-effect relationship. *Id.* The report's primary author, Patrick Grother, stated that the test demonstrates "empirical evidence for the existence of demographic differentials in the majority of the face recognition algorithms," yet the study's authors "do not explore what might cause these differentials" and instead publish the report in hopes that its data will be considered by policymakers, developers, and other decision-makers to make informed choices about using this software. *Id.*

[100] *See* GARVIE ET AL., *supra* note 2, at 54 (providing potential causes for the differences in error rates amongst different demographics); Abrar Al-Heeti, *Amazon's facial tech shows gender, racial bias, MIT study says*, CNET (Jan. 25, 2019), *archived at* https://perma.cc/8PZA-2WZ9 (reporting on the race and gender differentials in Amazon's software specifically). The MIT Media Lab study provided empirical data that "Amazon's facial technology had a harder time recognizing the gender of darker-skinned women and made more mistakes identifying gender overall than competing technologies from Microsoft and IBM," and specifically, "Amazon's Rekognition software incorrectly identified women as men 19 percent of the time" and "it incorrectly identified darker-skinned women as men 31 percent of the time" while "[s]oftware from Microsoft, by comparison, identified darker-skinned women as men 1.5 percent of the time." Al-Heeti, *supra*.

[101] *See* GARVIE ET AL., *supra* note 2, at 54 (noting a social trend and gender norm as a potential factor in a hypothetical algorithm's inability to identify women at a lower rate of accuracy).

individuals with darker skin tones.[102] Another potential explanation for algorithm bias may be related to the databases themselves—if the training data is not a diverse collection of images, the algorithm will naturally be less reliable for members of a demographic that is not adequately represented.[103] These observations shed doubt upon the reliability of current systems, and also impose challenges upon software developers who are attempting to train new algorithms.[104]

C. Bans at the Local Level: Municipalities Prohibiting Police Use of Facial Recognition Technology

There are currently no federal restrictions upon the government's use of facial recognition for policing.[105] All prior attempts to pass federal legislation focusing on facial recognition have not succeeded, effectively delegating the authority to state and local governments.[106] In 2016, as part of its study confronting the dangers

[102] *See id.* (providing a potential scientific reason for algorithms' higher rates of inaccuracy in identifying dark-skinned people).

[103] *See id.* at 56 (acknowledging that the demographic differential could also be caused by a non-diverse or small dataset used to train the algorithm); *see also* Elizabeth Fernandez, *Facial Recognition Violates Human Rights*, *Court Rules*, FORBES (Aug. 13, 2020), *archived at* https://perma.cc/26NG-A7WF (exemplifying that an algorithm "trained on a data set comprising of mostly white males, it's going to become really good at identifying white males.").

[104] *See* Fernandez, *supra* note 103 (emphasizing the crucial foundational problems that arise when systems are based on a non-diverse collection of images); FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT, *supra* note 57, at 5 (recognizing that one of the major factors contributing to an algorithm's accuracy is "the data used to 'train' the system to compare and match images (e.g., the amount of images used; the demographics of the persons in the images compared; and whether the composition of images in the training data set is representative of the population whose images may be compared using the system once deployed.")").

[105] *See* Metz, *supra* note 70 (explaining that there is some deference to local legislators in determining what kinds of restrictions or bans they would like to impose on their law enforcement agencies); Sam DuPont, *Facial Recognition Is Here But We Have No Laws*, NEXTGOV (July 8, 2020), *archived at* https://perma.cc/H56H-XWD5 (describing how the lack of national legislation has forced state and local governments to take initiative to protect their citizens).

[106] *See* Alfred Ng, *Lawmakers propose indefinite nationwide ban on police use of facial recognition*, CNET (June 25, 2020), *archived at* https://perma.cc/FN2H-6AD8 (stating that "[m]embers of Congress have introduced several bills that tackle facial recognition in different ways, including a ban in public housing and requiring consent from businesses that use the technology . . ." but "[n]o federal laws on facial

of facial recognition, the Center on Privacy & Technology at Georgetown Law drafted model legislation adaptable for either Congress or a state legislature.[107] The proposal enumerates specific allowed instances for governmental use and delineates several exceptions to limit each scenario.[108] Since releasing the model legislation, the same researchers have revised their stance on such a regulatory framework; in 2018, they released a statement calling for a more stringent ban on the technology.[109] Since there are no set boundaries delineating where, when, and how facial recognition can be used as a tool for law enforcement, local municipalities have the liberty to decide whether they will prohibit or limit these applications.[110] In May 2019, San Francisco became the first United

recognition have passed, leaving state and local officials to pass their own regulations on the technology."). *See also* Khari Johnson, *Congress moves toward facial recognition regulation*, VENTUREBEAT (Jan. 15, 2020), *archived at* https://perma.cc/MU4U-DRFN (expressing how facial recognition regulation has historically been a bipartisan issue, as evidenced by the 2019 bill led by Democratic Representative Elijah Cummings and Republican Representative Jim Jordan). This legislation, however, faced obstacles following the death of Rep. Cummings and the focus on pressing Congressional issues such as impeachment. *Id.*

[107] *See* GARVIE ET AL., *supra* note 2, 102–19 (creating a model for federal and state legislatures to adopt as a means of implementing a regulatory framework upon an increasingly-powerful technological tool). The legislation provides a model for federal law enforcement which focuses on "all federal and state law enforcement (1) access to all arrest photo databases and driver's license and ID photo databases, and (2) use of real-time face recognition." *Id.* at 102. The model state legislation is identical except for the fact that it additionally seeks to control state law enforcement access to arrest photo databases. *Id.*

[108] *See id.* at 103–15 (listing specific allowed uses and imposing strict limitations to prevent abusive tactics).

[109] *See* Garvie & Moy, *supra* note 65 (demonstrating a reversal in expert opinion on appropriate uses of facial recognition). A group consisting of some of the same researchers adopted a much less inclusive view on facial recognition by rejecting the proposals written in the previous study in favor on an outright ban. *Id.* Their statement, referencing the 2016 report calling for "common sense legislation" to regulate law enforcement's use of the technology, rejected their previous recommendations in favor of a moratorium or ban. *Id.* The researchers attribute this shift in perspective to "a dramatic range of abuse and bias" that has occurred in the interim period. *Id.* Specifically, they mention the Baltimore County Police Department's use of the technology to identify and arrest protesters in the aftermath of Freddie Gray's death, the false identification of a Brown University student as a potential terrorist suspect, and extensive research that speaks to the existence of extreme algorithmic biases. *Id.*

[110] *See* Metz, *supra* note 70 (further noting that municipalities have the power to ban or regulate at a local level); Garvie & Moy, *supra* note 65 (recommending that local

States city to impose a ban on the use of facial recognition technology by government agencies.[111] Several other local governments instituted bans within the next year, including Portland, Oregon.[112] This ban, announced in September 2020, was the broadest regulatory legislation of its kind passed by a city, as it prohibited both governmental and commercial implementations of the technology.[113] The mayor of the city announced that concern surrounding the surveillance of protests occurring in the wake of the police killing of George Floyd served as an impetus for the sweeping ban.[114]

Lawmakers have also begun to introduce legislation to federally ban the use of such technology by all federal agencies, absent Congress's explicit permission.[115] In June 2020, several Democratic senators and representatives proposed the Facial Recognition and Biometric Technology Moratorium Act ("Facial Recognition

municipalities feel empowered to place a moratorium on police use of facial recognition to better curb its use, considering that there is still a lack of federal legislation).

[111] *See* Kari Paul, *San Francisco is first US city to ban police use of facial recognition tech*, THE GUARDIAN (May 19, 2019), *archived at* https://perma.cc/D5TE-TW9Q (reporting on the significance of such a ban, especially in a city regarded as a tech hub); Conger et al., *supra* note 12 (explaining how the decision, which came to fruition after an 8-to-1 vote by the Board of Supervisors, effectively banned law enforcement's use of facial recognition in one of the first major U.S. cities). Aaron Peskin, one of the bill's sponsors, was quoted as saying: "San Francisco being the real and perceived headquarters for all things tech also comes with a responsibility for its local legislators." Conger et al., *supra* note 12.

[112] *See* Metz, *supra* note 70 (detailing Portland, Oregon's implementation of a facial recognition ban).

[113] *See id.* (describing the reasons why Portland's ban was especially groundbreaking). This ban, unlike most bans of its kind implemented in local and state governments, banned facial recognition in both governmental and commercial contexts. *Id.* Most other bans focus on governmental uses. *Id.*

[114] *See id.* (reporting that "Portland Mayor Ted Wheeler expressed . . . concern that facial-recognition technology could be used to surveil protestors"); *see also* Lauren Valenti, *Can Makeup Be an Anti-Surveillance Tool?* VOGUE (June 12, 2020), *archived at* https://perma.cc/B5CP-HPMQ (describing methods of makeup application used by protestors in support of the Black Lives Matter movement to conceal their identities from law enforcement).

[115] *See* Aaron Boyd, *Lawmakers Introduce Bill to Ban Federal Use of Facial Recognition Tech*, NEXTGOV (June 26, 2020), *archived at* https://perma.cc/9DR8-4DPL (detailing the efforts of a group of bicameral Democratic lawmakers to impose regulations at the federal level).

Moratorium Act").[116] The legislation intends to serve as an all-encompassing ban on biometric surveillance systems implementing facial recognition, and, if passed, would prohibit both federal funding of such systems and the use of evidence obtained through these methods in judicial proceedings.[117] Rather than naming instances in which the technology should not be implemented, the bill bans its general use and carves out exceptions for laws which would allow it only in extreme circumstances and with a great degree of caution and care.[118]

In addition to legislative pushback, several top vendors and tech companies have suspended the sale of their software to law enforcement agencies.[119] Amazon announced a one-year moratorium

[116] *See id.* (naming the act brought forward by Senators Edward Markey and Jeff Merkley and Representatives Pramila Jayapal and Ayanna Pressley). *See also* Facial Recognition and Biometric Technology Moratorium Act of 2020, S. 4084, 116th Cong. (2019–2021), *archived at* https://perma.cc/SPM8-59S5 [hereinafter Moratorium Act of 2020] (presenting the key information relating to the proposed legislation).

[117] *See id.* (describing the goals of the proposed legislation). With regard to federal agencies, the bill calls for a blanket ban on biometric surveillance systems that implement facial recognition technology or "information derived from a biometric surveillance system operated by another entity," such as another authorized federal agency or through a contracted vendor of the software. *Id.* The bill's language also calls for the prevention of any federal funds being used for the purchase of biometric surveillance systems, as well as prohibiting the federal government from giving grant money to state or local agencies, unless that organization is similarly regulated. *Id.* The bill additionally prevents use of information collected in violation of this law in judicial proceedings and also grants citizens a right to action. *Id.*

[118] *See* Olivia Solon, *Facial recognition bill would ban use by federal law enforcement*, NBC NEWS (June 25, 2020), *archived at* https://perma.cc/32AY-NV7N (summarizing that "[t]he bill states that this type of surveillance technology could only be used if there was a federal law with a long list of provisions to ensure it was used with extreme caution."). Furthermore, the bill provides that

> [a]ny such federal law would need to stipulate standards for the use, access and retention of the data collected from biometric surveillance systems; standards for accuracy rates by gender, skin color and age; rigorous protections for due process, privacy, free speech, and racial, gender and religious equity; and mechanisms to ensure compliance with the act.

Id.

[119] *See* Levy & Hirsch, *supra* note 49 (addressing Amazon's moratorium on its Rekognition software); Rebecca Heilweil, *Big tech companies back away from selling facial recognition to police. That's progress.*, VOX (June 11, 2020) [hereinafter Heilweil, *Big tech*], *archived at* https://perma.cc/BB4N-MJED (describing three tech giants' recent pushback against law enforcement's use of facial

on the sale of its software, Rekognition.[120] Similarly, IBM suspended its development of all facial recognition products, directly referencing the harm that could be caused by the technology's potential for abuse.[121] In the same vein, Microsoft announced that the company would refuse to sell its software to police agencies absent the passing of federal legislation.[122]

IV. Analysis

This section identifies the major concerns linked to government use of facial recognition technologies, identifies the

recognition). Despite the apparent progressivity demonstrated by these Big Tech companies, "critics of facial recognition technology have warned that corporate calls for regulation should be met with skepticism, as companies can push laws that are weak and ultimately defend their interests," further noting that "these companies are known to have extensive budgets for lobbying." Heilweil, *Big tech, supra*.

[120] *See id.* (noting Amazon's response to critiques of facial recognition). While the company ultimately placed a moratorium on the sale of its Rekognition software, Amazon allowed certain exceptions, stating that it will not discontinue use by organizations actively fighting human trafficking and locating missing children. *Id.*

[121] *See id.* (referencing IBM's decision to cease its production of facial recognition software); Rebecca Heilweil, *Why it matters that IBM is getting out of the facial recognition business*, VOX (June 10, 2020) [hereinafter Heilweil, *IBM*], *archived at* https://perma.cc/QE54-T973 (describing IBM's influential decision to discontinue its engineering of general-purpose facial recognition technology, citing its CEO's statement of the company's opposition to use of facial recognition technology "'for mass surveillance, racial profiling, [and] violations of basic human rights and freedoms.'").

[122] *See* Heilweil, *Big tech, supra* note 119 (conveying Microsoft's stance on the lack of regulation of facial recognition technology). Microsoft President Brad Smith indicated that the company would be refusing to sell its technology to police organizations absent a national regulatory law grounded in human rights. *Id. See also* Jay Greene, *Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM*, WASH. POST (June 11, 2020), *archived at* https://perma.cc/KRD4-4WKU (detailing Brad Smith's decision as well as the similar moves by IBM and Amazon, and how they struggled to strike a balance between their relationship with the Defense Department and their employees' resistance to working with law enforcement). Further, these tech companies faced pressure from critics of government use of the technology, such as MIT Media Lab researcher Joy Buolamwini, who compelled Microsoft, in particular, to "take a stand." *Id.*

current lack of federal regulatory legislation, and recommends a moratorium or outright ban to mitigate potential abuse.[123]

A. Constitutional Concerns: Invasion of Privacy and Destruction of Anonymity

The invasive nature of facial recognition presents a complex inquiry as to whether its use by law enforcement presents one or more constitutional violations.[124] Based on the rights delineated in the U.S. Constitution and by case precedent, it is inconclusive as to whether the Supreme Court would recognize certain government uses, such as police surveillance, as inherently unconstitutional.[125] However, such analysis of potential infringements is crucial to understanding the

[123] *See* discussion *infra*, Sections IV, A–D (providing examples of the negative implications of government use of facial recognition in the first two sections and critiquing and modifying current legislative approaches in the latter).

[124] *See* Hirose, *supra* note 1, at 1595 (describing how there is not yet case precedent regarding the constitutionality of facial recognition, and in fact, "higher courts are still in the process of deciding if and how the Fourth Amendment applies to surveillance technologies that have now been in use for decades, like cell phone location tracking, prolonged video surveillance, and license plate readers."); FACING THE FUTURE OF SURVEILLANCE, *supra* note 80, at 16 (recognizing the grave Constitutional concerns that are linked to facial recognition in the hands of government agencies).

> Facial recognition technology creates unprecedented potential to monitor individuals, and thus unprecedented questions about how we should regulate surveillance technology. The technology takes one of the most basic human functions—the ability to recognize individuals by their appearance—and combines it with computer capabilities to act on a scale that would otherwise require massive amounts of human labor. This mix forces us to reconsider fundamental assumptions about how law enforcement can, and should, interact with individuals. It is critical that we carefully consider the impact on constitutional rights and principles, and proper limits of facial recognition surveillance, before allowing it to become a common law-enforcement tool.

FACING THE FUTURE OF SURVEILLANCE, *supra* note 80, at 16.

[125] *See* Hirose, *supra* note 1, at 1595 (explaining the complexity of the Fourth Amendment's application in this context). *See also* Nakar & Greenbaum, *supra* note 7, at 116 (recognizing the difficulty and ambiguity in assessing how the Constitution may be applied to the government's use of facial recognition).

dangers of what may otherwise be perceived as an efficient and effective tool for aiding law enforcement.[126]

While the word "privacy" is not explicitly mentioned in the U.S. Constitution, the Supreme Court's Fourth Amendment analysis holds that an individual has a right to privacy where there is an actual, subjective expectation of privacy and such an expectation is reasonable based on society's standards.[127] Those who advocate for a more limited application of the Fourth Amendment's protections express the inconsistency of supposedly maintaining a reasonable subjective expectation of privacy in their faceprint and appearing in public voluntarily.[128] Critics of surveillance tactics, however, express that an expectation of privacy in public spaces exists, often citing the landmark case *United States v. Katz*, which rejected previous notions

[126] *See* Hartzog, *supra* note 49 (warning that "facial recognition technology is a menace disguised as a gift. It's an irresistible tool for oppression that's perfectly suited for governments to display unprecedented authoritarian control and an all-out privacy-eviscerating machine."); Metz, *supra* note 70 (recognizing that advancements in surveillance technology formerly embraced and celebrated now typically elicit fearful reactions from the general public and those wary of the potential for government misuse).

[127] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (featuring a two-pronged analysis to establish whether a person has a privacy interest). The Court determined that "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id. See also* Aguado, *supra* note 14, at 208 (summarizing the Court's application of the Fourth Amendment to determine when an individual possesses a right to privacy, and recognizing the third-party doctrine, which removes any reasonable expectation of privacy from any information disclosed to a different party).

[128] *See* Hirose, *supra* note 1, at 1600 (demonstrating how the Court in *Katz*, for the first time, rejected the notion that there is not an existing right to privacy in public spaces). Instead, the *Katz* Court recognized that even in a publicly accessible area, something may be constitutionally protected so long as a person seeks to maintain its privacy. *Id.*

The takeaway from *Katz*, as expressed in later decisions analyzing the opinion and Justice Harlan's concurrence, "have explained that, under this approach, the Fourth Amendment protects legitimate or reasonable expectations of privacy where: (1) 'the individual, by his conduct, has exhibited an actual (subjective) expectation of privacy,' and (2) 'the individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable.'" *Id.* at 1601. This interpretation, which recognizes that there is merit to the notion that Americans have the right to protect their privacy in public spaces, seems to suggest that the *Katz* framework would offer protection against the government's use of facial recognition as a surveillance tactic. *Id.*

that a physical trespass was necessary for privacy violations, and established that "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[129] Furthermore, while it is true that appearing in public and therefore exposing one's face is a voluntary action, there is no reasonable alternative—normal day-to-day functioning requires entering into the public sphere.[130] Facial recognition's implementation exposes individuals to the threat of having their identifying information collected and stored by nature of merely appearing in public.[131] A faceprint's permanence and generally unchangeable nature makes individuals particularly vulnerable.[132] Resultingly, victims of a breach

[129] *See Katz*, 389 U.S. at 351 (explaining how the Court did not reject the idea of extending constitutional notions of privacy to individuals in public spaces); Hirose, *supra* note 1, at 1601 (reiterating that "most people today exhibit subjective and actual expectations of privacy in their identities even while they are out in public"). *See also* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (holding that "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere."). The Court's decision regarding law enforcement's use of historic cell-site location information expressed the notion that to "secretly monitor and catalogue every single movement" of an individual constituted a violation of society's expectations about the scope of law enforcement's authority. *Id.* at 2218. *See also* Garvie & Moy, *supra* note 65 (explaining how the surveillance tactics used in conjunction with facial recognition fall under the category of tracking that the Court condemned in its *Carpenter* analysis, and its use can potentially expose private associations central to a person's identity which should be entitled to protection).

[130] *See* Levashov, *supra* note 3, at 173 (noting the difficulty in avoiding being surveilled); Barrett, *supra* note 7, at 240 (providing that over 227 million Americans have driver's licenses, and several states allow facial recognition searches on those photo databases – a statistic that demonstrates how being subject to facial recognition searches is linked to certain unavoidable practices, such as having a driver's license).

[131] *See* Levashov, *supra* note 3, at 172 (expressing that "a person is vulnerable to having identifying information captured and stored by the government . . . just by appearing in public.").

[132] *See id.* at 173 (recognizing the sensitivity of a person's face as an identifier, stating that "[p]articularly troubling is the fact that a faceprint is generally permanent and unchangeable.").

> Once a person's faceprint has been acquired and stored in a database, any party with access to that database can link that person's likeness to his identity. Unlike assigned identifiers, such as credit card numbers, a faceprint cannot be changed if a security breach causes the data to fall into undesirable hands. Although the appearance of a person's face can change due to weight fluctuations, plastic surgery, or aging, future algorithms may be able to take such changes into account in determining matches.

involving facial recognition data cannot remedy the intrusion in a normal way such as changing a credit card number or account password—instead, they would have to take drastic measures such as cosmetic surgery.[133]

Introducing the threat of widespread biometric identification in surveillance tactics would effectively alter expectations of anonymity in public spaces.[134] This alteration, in turn, can indirectly stifle other individual freedoms by deterring people from exercising their rights in fear of constant governmental surveillance.[135] As facial recognition has become more widespread, this effect on assembly has already begun to appear concretely.[136] For example, during the nationwide protests in support of the Black Lives Matter movement, activists

Id. It is also important to note that what makes people particularly vulnerable is the fact that "a faceprint is generally permanent and unchangeable." *See id*. at 172. *See also What Facial Recognition Technology Means*, *supra* note 13 (indicating that unlike a password or a credit card, biometrics are not easily changed); Barrett, *supra* note 7, at 225 (differentiating faceprints from other identifiers by positing that the fact that "you can reset a password, but not your face, heightens the stakes of using faces as an identifier; it makes surveillance systems harder to evade, and breaches more consequential.").

[133] *See What Facial Recognition Technology Means*, *supra* note 13 (referencing the difficulty of changing one's faceprint relative to other sensitive information, like a credit card number).

[134] *See* Ringrose, *supra* note 5, at 63 (positing that "real-time face recognition will redefine public spaces by destroying anonymity"); Levashov, *supra* note 3, at 175 (noting that with the presence of "cameras scanning crowds at rallies, protests, bars and nightclubs, people may become fearful of acting in any way that they would not be comfortable revealing to the general public."); Nakar & Greenbaum, *supra* note 7, at 114 (conveying the importance of a person's presence in the public sphere, as it "reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."). The authors further provide specific examples: "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." Nakar & Greenbaum, *supra* note 7, at 114.

[135] *See* Fernandez, *supra* note 103 (quoting Stanley Shikuma's reasoning that "if you think that the police are watching you . . . when you go to the bank, or you go to the doctor's office, or you go to the church or the synagogue or the mosque, you'll be less likely to exercise those freedoms"). *But see* Nakar & Greenbaum, *supra* note 7, at 116 (analyzing how the Constitutional protection of anonymity is ambiguous and "far from absolute").

[136] *See* Fernandez, *supra* note 103 (recalling that privacy concerns "showed up in a concrete way during the Black Lives Matter protests . . . people were encouraged to not post images on social media of people who were at the protests.").

covered their faces and applied makeup to strategically alter their appearance and thwart identification, despite the constitutionally granted right to freedom of assembly.[137] As privacy and anonymity are fundamentally linked to the ability to exercise other democratic rights, the omnipresence of facial recognition poses a serious and very real threat.[138] Although the Supreme Court has not yet deliberated about whether government use of facial recognition technologies are fundamentally violative of constitutionally-granted rights, the high risks of mass surveillance substantially outweigh the potential benefits of their use.[139]

B. Algorithmic Bias Disproportionately Affects Certain Demographics

Beyond the essentially universal harms of widespread government use of facial recognition, the pervasive presence of algorithmic bias within most software creates a disproportionate effect against certain demographic groups of which the technology identifies

[137] *See* Valenti, *supra* note 114 (describing how protestors used makeup as an anti-surveillance effort). Protestors use these makeup designs as a method of resistance and in an attempt to protect their identities, but this method is certainly not foolproof. *Id.* For example, an individual's ears can be a distinguishing feature that could negate these attempts to avoid detection. *Id. See also* Barrett, *supra* note 7, at 243 (recognizing that "the knowledge that law enforcement is capable of quickly and cheaply identifying people in a crowd can deter political protest, as people may be correctly afraid of reprisals."); GARVIE ET AL., *supra* note 2, at 3 (noting that, of the fifty-two law enforcement agencies studied, only one explicitly prohibited officers from using facial recognition as a means of tracking individuals engaged in "political, religious, or other protected speech."); Folley, *supra* note 3 (detailing the Memphis police department's creation of a protestor "watch list"). According to reports from Memphis law enforcement agencies to a local news station, the police collect "intelligence containing vital information of BLM protesters – including date of birth, weight and height – to help create a 'watch list' that bars those listed from entering the Memphis City Hall without an escort." Folley, *supra* note 3.

[138] *See* Barrett, *supra* note 7, at 244 (acknowledging that the threats facial recognition technologies pose to the "democratic rights of free assembly, expression, and political dissent are concrete, severe, and broadly applicable.").

[139] *See* Hirose, *supra* note 1, at 1595 (describing how "higher courts are still in the process of deciding if and how the Fourth Amendment applies to surveillance technologies that have now been in use for decades, like cell phone location tracking, prolonged video surveillance, and license plate readers."); *see also* LEARNED-MILLER ET AL., *supra* note 23, at 3 (stating that the potential benefits of a powerful technological tool "are tempered with risks of mass surveillance, disparate impact on vulnerable groups, algorithmic bias, and lack of affirmative consent.").

with much less accuracy.[140] The assumption of machine neutrality is false—the algorithms reflect the biases of their human coders.[141] Research indicates that these algorithms are inherently biased in the accuracy of their performance especially affecting individuals with dark skin, women, transgender and non-binary individuals, elderly people, and young children, fostering an unequal power dynamic.[142] Other differentials between demographics also pose such an imbalance.[143] For example, people of color are more frequently

[140] *See* Barrett, *supra* note 7, at 240 (claiming that the threat of surveillance is essentially harmful to all members of society).

> Facial recognition technologies inflict what can be described as quasi-universal harms by virtue of the fact that they are a dragnet surveillance tool — anyone with a picture in a government database, who posts a picture on a commercial internet service, or ventures outside in public with their face uncovered is implicated. The term "universal" risks implying that the harms of facial recognition are equally dispersed when they are not — populations that were already more vulnerable to surveillance and over-policing are much more susceptible.

Id. at 247. *See also* Ringrose, *supra* note 5, at 62 (indicating that the technology's shortcomings can amplify already-present differences between demographic groups).

[141] *See id.* (reiterating that software will "reflect the priorities, preferences, and prejudices of their coders, and this 'coded gaze' leads to tangible negative effects for African Americans," a demographic on which facial recognition technologies tend to have far higher error rates); GARVIE ET AL., *supra* note 2, at 51 (acknowledging that the size and diversity of a dataset is a major factor influencing the ability for an algorithm to perform accurately and consistently on different demographic groups). While it may seem natural to assume that artificial intelligence provides a means of avoiding human bias and attaining neutrality, these biases are included in the code of the algorithm and are therefore still very much a threat. GARVIE ET AL., *supra* note 2, at 56.

[142] *See* Ovide, *supra* note 13 (recognizing that institutionalized factors cause an imbalance in the sense that even 100% accurate facial recognition can still be implemented in a way that disproportionately affects certain groups of people); Barrett, *supra* note 7, at 247–48 (describing how most algorithms fail to perform with the same level of accuracy for all demographics). These groups include "people with darker skin, women, transgender and non-binary individuals, the elderly, and . . . children." Barrett, *supra* note 7, at 247–48.

[143] *See* Ringrose, *supra* note 5, at 62 (arguing that the "false assumption of machine neutrality" can cause a legitimate threat to civil rights). *See also* Al-Heeti, *supra* note 100 (reporting on the shortcomings of Amazon's Rekognition software specifically). An MIT study demonstrated the interaction between race and gender as two of the major variables that cause discrepancies in the software's ability to perform accurately. *Id.* Specifically, "Amazon's facial technology had a harder time

arrested for small crimes and are therefore more likely to appear in databases.[144] Furthermore, Black and Native American people, for instance, have disproportionately high rates of incarceration.[145] These facts indicate that the biases present in the majority of facial recognition systems will exacerbate the structural inequalities within the criminal justice system.[146] The presence of these discrepancies in accuracy are built into the software and can manifest error in several ways, with varying levels of risk.[147] While a false negative or false positive can have minute effects in the context of, for instance, an improper misidentification within a personal photo gallery, the possibility of wrongfully identifying a criminal suspect presents a much graver consequence of algorithmic bias.[148] Facial recognition systems should not be implemented by police forces if such systems' accuracy differs significantly between demographics.[149]

recognizing the gender of darker-skinned women and made more mistakes identifying gender overall than competing technologies from Microsoft and IBM." *Id.*

[144] *See* Fernandez, *supra* note 103 (noting that higher arrest rates for people of color would cause their faces to be more likely to appear in databases); Hirose, *supra* note 1, at 1616 (explaining that despite the requirement of reasonable suspicion in police stops, "people of color have been stopped disproportionately and discriminatorily targeted by the police.").

[145] *See* Barrett, *supra* note 7, at 249 (providing that Black and Native American populations are incarcerated and killed by police at a higher frequency than that of other demographics).

[146] *See id.* at 247 (acknowledging the disproportionate effects of bias expected to be experienced by certain populations).

[147] *See* LEARNED-MILLER ET AL., *supra* note 23, at 36 (listing examples of low-risk uses of facial recognition, such as sorting a personal photo collection; medium-risk examples, such as for medical diagnosis purposes; and high-risk examples, such as in conjunction with police body-worn cameras).

[148] *See id.* (exemplifying the concern of using facial recognition in scenarios that would be classified as high-risk).

[149] *See* Hirose, *supra* note 1, at 1618 (advocating that the disparate impact to be experienced by different classes of people demonstrates the dangers of implementing facial recognition systems). A specific example manifests "[w]ith the number of outstanding warrants and tickets, which themselves are known to disproportionately and unfairly impact communities of color, the suspicionless use of facial recognition to identify person's outstanding warrants and tickets will result in an exponential increase in the number of people who are" stopped by police on a daily basis. *Id.*

C. Legislation Gaps

Presently, there is no existing federal legislation which explicitly confronts the collection of faceprints in databases.[150] However, as governmental implementation of facial recognition technologies has become widespread and research overwhelmingly demonstrates the presence of accuracy bias, a number of municipalities have chosen to issue legislation banning or severely regulating its use.[151] The lack of a uniform stance on banning or regulating the technology presents an unclear, hazardous atmosphere in the United States, leading to nationwide inconsistencies and ambiguity.[152] In 2016, one group of researchers at Georgetown University's Center for Privacy & Technology drafted a comprehensive proposal for model legislation, which specifically delineates instances of acceptable government usage and proposes accountability for any instances of misuse—however, closer scrutiny toward the unique perils of facial recognition favors a more restrictive approach to regulation.[153]

1. Existing and Proposed Legislation

Much of the existing and proposed regulatory framework seeks to procedurally limit use by advocating for requirements such as

[150] *See* Levashov, *supra* note 3, at 176 (noting that, at the moment, "no federal law explicitly addresses the collection and storage of faceprints"); FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT, *supra* note 57 (acknowledging that "to date, there is no federal framework specifically directed at the development and use of FRT by government and private entities.").

[151] *See* Metz, *supra* note 70 (listing various U.S. cities and states that have chosen to implement a ban or moratorium).

[152] *See id.* (explaining that the government tends to defer to the state regarding such regulations). Due to the fact that sweeping federal legislation has been unsuccessful, and "no federal guidelines exist to limit or standardize the use of such surveillance technology . . . municipalities are left to decide for themselves what, if anything, to do to control its use." *Id.*

[153] *See* GARVIE ET AL., *supra* note 2, at 102 (providing detailed and exhaustive model legislation intended to be adapted for federal or state use). The model legislation, published in 2016 as an accompaniment to the researcher's detailed assessment of the dangers of government use of facial recognition technology, comprehensively addressed the several glaring opportunities for misuse. *Id. See also* Garvie & Moy, *supra* note 65 (indicating that researchers have since advised against implementation of the Center for Privacy & Technology's model legislation, instead advocating for a temporary moratorium until the presence of algorithmic bias is less of a disproportionate threat to certain demographics).

informed consent, prohibiting mass storage for extensive periods of time, creating an overseeing body, providing a private right of action for cases of misuse, and prioritizing data security to prevent breaches of sensitive information.[154] In recognition of the benefits of the technology, carving out exceptions in which use may be authorized appears to be a feasible alternative to prohibiting use entirely.[155] While many of these proposals provide intricately-detailed suggestions for restrictions, they do not consider the high risk and sensitivity of collecting a biometric so central to a person's identity.[156] An example of this is the aforementioned model legislation proposed by the Georgetown Law Center on Privacy & Technology.[157] While detailed in its approach to considering potential constitutional and human rights violations, the hypothetical legislation ultimately underestimated the potential for abuse still possible within its framework.[158] The deadly

[154] *See* LEARNED-MILLER ET AL., *supra* note 23, at 8 (expressing the importance of requiring informed consent for appropriate government use and proposing the creation of a new federal office for regulatory purposes); Hartzog, *supra* note 49 (noting that the Electronic Frontier Foundation's report recommends "restrictions on collecting and storing data; recommending limiting the combination of one or more biometrics in a single database; defining clear rules for use, sharing, and security; and providing notice, audit trials, and independent oversight.").

[155] *See* Levashov, *supra* note 3, at 190 (advocating a less extreme stance by positing that since "some state agencies, such as the DMV, may need to use facial recognition technology to prevent fraud, the practice of using the technology in government functions should not be prohibited entirely."); Klosowski, s*upra* note 4 (weighing the benefits of such an advanced software in several contexts). Proponents of FRT praise the software's ability to identify potential suspects and monitor crowds at large events for security purposes. Klosowski, *supra* note 4. Those generally in favor of the software also reference the convenience and efficiency guaranteed by such a tool, even in everyday contexts such as for the organization of personal photos, securing personal electronic devices, and acting as an accessibility tool for the blind and visually impaired communities. *Id.*

[156] *See* Hartzog, *supra* note 49 (expressing the cruciality of understanding the sensitivity of maintaining privacy in one's faceprint).

[157] *See* GARVIE ET AL., *supra* note 2, at 102–19 (delineating specific instances of acceptable and unacceptable governmental uses of facial recognition technology, advocating for transparency and audits, among other regulatory requirements).

[158] *See* Garvie & Moy, *supra* note 65 (stating a new perspective endorsed the Georgetown Center for Privacy & Technology, revising the previous publication advocating for regulation in favor of a sweeping ban, in light of new research and evidence of abusive implementation).

> In 2016, the Center on Privacy & Technology issued a report on police use of face recognition technology in the United States. In that report we recommended that state legislatures adopt common sense legislation to comprehensively regulate law enforcement use

combination of extreme surveillance measures and the threat of disparate treatment among demographics suggests that regulated use should be the exception rather than the rule; government use of the technology should be banned in the absence of either exigent or inherently low-risk circumstances.[159] In June 2020, a group of federal lawmakers introduced a bill, the Facial Recognition Moratorium Act, with the goal of prohibiting surveillance by means of facial recognition.[160] This Congressional action did not pass, but its introduction, along with the existing patchwork of legislation, demonstrates the need for laws explicitly outlining a consistent framework.[161]

2. Why is a Moratorium or Ban Necessary?

The dichotomous nature of digital technologies typically forces society to strive to find a balance between innovation and abuse; however, facial recognition must be regarded as fundamentally dangerous given the extreme measures necessary to thwart its

> of face recognition. Since then, a dramatic range of abuse and bias has surfaced. Baltimore County Police used the technology to identify and arrest people protesting the death of Freddie Gray. A Brown University student was falsely identified as a possible terrorist suspect responsible for attacks in Sri Lanka. Research by Joy Buolamwini, Timnit Gebru, and the ACLU of Northern California verified that the technology still exhibits race and gender bias. As a result, we now believe that state, local, and federal government should place a moratorium on police use of face recognition. We also believe that jurisdictions that move to ban the technology outright are amply justified to do so.

Id.

[159] *See* Hartzog, *supra* note 49 (supporting the idea of banning facial recognition technologies rather than proposing regulatory legislation).

[160] *See* Boyd, *supra* note 115 (reporting on the 2020 bill proposing a federal ban). This bill was introduced in June 2020 by a group of Democratic lawmakers, namely Senator Edward Markey of Massachusetts, Senator Jeff Merkley of Oregon, Representative Pramila Jayapal of Washington, and Representative Ayanna Pressley of Massachusetts. *Id.* The Bill's objective was "[t]o prohibit biometric surveillance by the federal government without explicit statutory authorization and to withhold certain federal public safety grants from state and local governments that engage in biometric surveillance." *Id.*

[161] *See id.* (summarizing the key issues prompting lawmakers to propose a ban). *See also* Moratorium Act of 2020, *supra* note 116 (recording key information about the status of the bill and recognizing that the bill failed to be signed into law).

exploitation.[162] Facial recognition is not the only technology that can be used nefariously—geolocation data, search history data, and even other types of biometrics may also be abused—however, these technologies have been successfully regulated to mitigate their potential for misuse.[163] Yet facial recognition is uniquely concerning due to several distinguishable characteristics.[164] The face is central to identity, difficult to hide and change, and unlike other sensitive sources of information, cannot be encrypted.[165] The present existence of name and face databases exacerbates the potential for exploitation.[166] Most crucially, the confirmation that the technology still exhibits race and gender bias, the effects of which have already manifested, reinforces

[162] *See* Boyd, *supra* note 115 (quoting Rep. Ayanna Pressley) (describing facial recognition technology as a system that is "fundamentally flawed, systematically biased, and has no place in our society").

[163] *See* Hartzog, *supra* note 49 (explaining why facial recognition requires unique precautions).

> Despite the problems our colleagues have documented, you might be skeptical that a ban is needed. After all, other technologies pose similar threats: geolocation data, social media data, search history data, and so many other components of our big data trails can be highly revealing in themselves and downright soul-searching in the aggregate. And yet, facial recognition remains uniquely dangerous. Even among biometrics, such as fingerprints, DNA samples, and iris scans, facial recognition stands apart.

Id.

[164] *See id.* (listing distinct examples as to facial recognition's distinguishable qualities which pose a danger to society).

[165] *See What Facial Recognition Technology Means*, *supra* note 13 (stating that "biometric information is already among the most sensitive of our private information, mainly because it is both unique and permanent. You can change your password. You can get a new credit card. But you cannot change your fingerprint, and you cannot change your face.").

> Once someone has your faceprint, they can get your name, they can find your social networking account, and they can find and track you in the street, in the stores that you visit, the Government buildings you enter, and the photos your friends post online. Your face is a conduit to an incredible amount of information about you, and facial recognition technology can allow others to access all of that information from a distance, without your knowledge, and in about as much time as it takes to snap a photo.

Id. *See also* Hartzog, *supra* note 49 (describing how faceprints are central to identity).

[166] *See id.* (recognizing the fact that there are already databases in existence which match names and faces, such as driver's license logs, mugshot collections, and social media profiles, which puts sensitive information at a further risk of data breach).

the need for either a federal ban or moratorium.[167] Even in the event that all algorithmic biases are fully eliminated, implementation of facial recognition in the hands of law enforcement still bears many risks, and in the absence of a permanent ban, any use should ideally be fully transparent and limited in scope to mitigate the level of surveillance that will inevitably ensue as technology continues to develop and become more ubiquitous.[168]

V. Conclusion

Constitutional notions of privacy have undergone a metamorphosis as extraordinary technological advancement has allowed government agencies to challenge traditional boundaries. Privacy, at its core, is not about maintaining secrecy, but rather, about maintaining control. Facial recognition is the last frontier for government surveillance—there is no separation between a person's identity and their faceprint. Oftentimes the discourse surrounding privacy is relative to its tension with safety concerns; violations of privacy are more palatable when they are serving a greater interest of public welfare. Yet the uniquely sensitive nature of a faceprint demonstrates just how nefarious facial recognition can be, when used as a means of governmental surveillance. This sensitivity, exacerbated by the presence of algorithmic bias, poses far too serious of a threat of misuse. A nationwide ban of government use of facial recognition is presently the only available option to protect citizens against the state's monitoring of the totality of human activity in public spaces.

[167] *See* Garvie & Moy, *supra* note 65 (revising Georgetown Law's previous stance on regulating use in favor of a stricter moratorium).

[168] *See* Hartzog, *supra* note 49 (expressing the viewpoint that restrictive legislation will be ineffective in preventing the transition to a surveillance-based society). *See also* LEARNED-MILLER ET AL., *supra* note 23, at 7 (advocating for core principles such as limited scope, informed consent, and prohibition of use in high-risk scenarios).