A NEW AGE OF SURVEILLANCE: FACIAL RECOGNITION IN POLICING AND WHY IT SHOULD BE ABOLISHED

Annslee Perego[†]

TABLE OF CONTENTS

I. INTRODUCTION

In an article Robert Williams wrote for the Washington Post in June 2020, he stated, "I never thought I'd have to explain to my daughters why Daddy got arrested."[1] How does one explain to two little girls that a computer got it wrong, but the police listened to it anyway?"[2] Williams, an

† Annslee Perego graduated from Baylor University in 2019 with a Bachelor of Social Work. She is a current student at Benjamin N. Cardozo School of Law where she is a Pro Bono Scholar and serves as the Editor-in-Chief of Volume 28 of the Cardozo Journal of Equal Rights and Social Justice. After graduating in May of 2022, she hopes to pursue a career in counterterrorism, cryptocurrency, data, or criminal law fields.

Annslee would like to specifically thank Professor Ngozi Okidegbe for her wise counsel while writing this note and encouragement throughout the process.

[1] Robert Williams, *I was wrongfully arrested because of facial recognition. Why are police allowed to use it?*, WASH. POST (June 24, 2020 3:04 PM), https://www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology/.

[2] *Id.*

African American male, was presented with an arrest warrant for felony larceny and detained in front of his wife and daughters after arriving home from work.[3] He was held for thirty hours before police realized that facial recognition software wrongfully identified Williams as the suspect.[4] A store owner had sent blurry surveillance footage of a black male stealing watches to the Detroit Police Department.[5] The footage was then sent to the Michigan State Police department where facial recognition software connected the store owner's grainy footage to an old driver's license picture of Williams.[6] Williams only found out that it was facial recognition technology that had led to his wrongful arrest when an officer slipped that the "computer must have gotten it wrong."[7]

Facial recognition, at its core is "the automated process of comparing two images of faces to determine whether they represent the same individual."[8] The use of facial recognition in policing has become more popular, because police are looking for alternatives to witness testimony that offer increased reliability, as "troubling" witness testimony has been facial recognition's "selling point."[9] The Federal Bureau of Investigation (FBI) has developed its own facial recognition software through its Next Generation (NGI) system, and enables police to use the system as well by submitting probe photos.[10] Additionally, police departments use other third party systems, such as Amazon's Rekognition, to employ facial recognition in their work.[11]

Current scholarship directs attention to the recent implementation of facial recognition in law enforcement, calling its use the beginning of a *1984* George Orwell "Big Brother" totalitarian society, and urging Congress to

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] *Face Recognition and Driver's License Photo-Sharing*, NAT'L IMMIGRATION LAW CENTER (Oct. 2019), https://www.nilc.org/issues/drivers-licenses/face-recognition-and-dl-photo-sharing/.

[9] Shira Ovide, *When the Police Treat Software like Magic*, N.Y. TIMES (June 25, 2020), https://www.nytimes.com/2020/06/25/technology/facial-recognition-software-dangers.html#:~:text=The%20arrest%20of%20a%20man,dangers%20of%20facial%20recognition%20technology.

[10] FBI, *Next Generation Identification (NGI)*, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi (last visited Sept. 18, 2020).

[11] Shirin Gaffary, *How to avoid a dystopian future of facial recognition in law enforcement*, Vox (Dec. 10, 2019, 8:00 AM), https://www.vox.com/recode/2019/12/10/20996085/ai-facial-recognition-police-law-enforcement-regulation.

create regulatory laws before the technology becomes too powerful.[12] Others warn that "the right to privacy has been substantially eroded by new technologies," arguing that facial recognition further diminishes individual privacy.[13] Apart from exploring the possibility that facial recognition technology will become too powerful through its potential to surveil citizens' everyday lives, as well as its role in diminishing privacy, there is little to be said about actual policies that Congress should implement to curtail these negative effects. This Note will focus on problems that facial recognition use already presents, as well as offer suggestions for limiting its use. For helpful reading, this Note will only engage in a discussion of use of facial recognition technology by United States law enforcement and will not address its use in other arenas such as national security.

One argument in favor of facial recognition use is the potential to improve efficient policing by providing leads to suspects in investigations. Currently the New York Police Department (NYPD) uses face recognition to identify potential suspects captured on camera at crime scenes.[14] In 2019, the NYPD's use of facial recognition technology resulted in "possible matches in 68 murders, 66 rapes, 277 felony assaults, 386 robberies, and 525 grand larcenies."[15] Although the technology improves efficiency, its use is currently problematic. For example, facial recognition technology has proven to "misidentif[y] people of color more often than white people,"[16] but is still being used in a largely unchecked manner. In addition to racial bias, the erosion of privacy along with concerns about the transparency of the use of the data derived from facial recognition software is problematic, further exacerbating minority groups' already diminished privacy.[17] Finally, the use of facial recognition in policing dilutes democratic participation, such as discouraging free speech among minorities.[18]

---

[12] Samuel D. Hodge, *Big Brother is Watching: Law Enforcement's Use of Digital Technology in the Twenty-Frist Century*, 89 U. CIN. L. REV. 30 (2020).

[13] 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 (2017).

[14] *NYPD Questions and Answers Facial Recognition*, NYPD, https://www1.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page.

[15] *Id.*

[16] Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use*, WASH. POST (Dec. 19, 2019, 6:43 AM), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

[17] Angelique Carson, *When surveillance perpetuates institutional*, IAPP (Apr. 13, 2016), racismhttps://iapp.org/news/a/when-surveillance-perpetuates-institutional-racism/.

[18] *See,* Aristos Georgiou, *Black Lives Matter Activist Hunted by NYPD Facial Recognition Technology*, NEWSWEEK (Aug. 15, 2020, 10:57 AM), https://www.newsweek.com/black-lives-matter-activist-hunted-facial-recognition-technology-1525335.

Considering these problems in conjunction with the expanding use of facial recognition technology in law enforcement, that has risen to "a level of prominence,"[19] facial recognition technology must be abolished in order to protect against the unfair use of the technology. If not completely abolished, the use of facial recognition needs to be, at the very least, limited. This Note will argue that its use in criminal prosecutions should be regulated, prohibited in use for real time facial recognition, and a singular, regulated facial recognition software should be used amongst all agencies. However, even if these suggestions were implemented, arrests like Robert William's[20] would still not be prevented since the technology itself is flawed and misidentifies innocent people.

Part I of this Note will provide an overview of the use of facial recognition. It will explore how facial recognition technology works and explain what systems law enforcement agencies are currently using ending with a brief overview of current legislation and legal landscape concerning facial recognition. Part II will analyze the various challenges that facial recognition presents. This part will explain that facial recognition is racially biased because it mismatches minorities at a higher rate than whites[21] and exacerbates racist policing. It will also highlight that police have little recourse for mistakes from facial recognition false positives like in Robert Williams's wrongful arrest.[22] Additionally, Part II will explain how facial recognition continues to erode privacy and show that there is little transparency in knowing how the data gained front the systems will be used, especially with law enforcement agencies using a variety of facial recognition software created by third parties such as Amazon, Microsoft, and IBM.[23] The section will also discuss how difficult gaining more transparency will be due to trade secret privilege that is meant to "safeguard[] [companies] from the competitive disadvantages that could result from disclosure."[24] Finally, Part II explains how facial recognition erodes democratic participation such as when people were discouraged from protesting out of fear of being facially

[19] Kirril Levashov, *The Rise Of A New Type Of Surveillance For Which The Law Wasn't Ready*, 15 COLUM. SCI. & TECH. L. REV. 164 (2013).

[20] Williams, *supra* note 1.

[21] Harwell, *supra* note 16.

[22] Williams, *supra* note 1.

[23] Karen Hao, *The two-year fight to stop Amazon from selling face recognition to the police*, MIT TECHNOLOGY REVIEW (June 12, 2020), https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/.

[24] US DOJ, *FOIA Guide, 2004 Edition: Exemption 4*, https://www.justice.gov/oip/foia-guide-2004-edition-exemption-4 (last visited Oct. 25, 2020).

recognized after the New York Police Department (NYPD) used facial recognition to surveille a Black Lives Matter ("BLM") protest leader.[25]

Part III will discuss proposed solutions to these problems such as limiting the use of facial recognition evidence in criminal prosecutions, advocating for a single, regulated system used among all agencies, and banning real time facial recognition. However, this section will also explain how none of these measures will be sufficient to create equitable use of facial recognition. After refuting the proposed solutions, Part IV will then conclude with why facial recognition should therefore be abolished within policing in order to protect against racial bias, privacy concerns, and loss of democratic participation. Until the major problems with facial recognition can be absolved, it should not be used at all.

II. BACKGROUND

Currently, "[p]olice departments are relying on facial recognition technology to facilitate arrests, charges, detentions, and criminal convictions,"[26] while the FBI also uses its own technology, Next Generation Identification (NGI), to effectuate its investigations.[27] Although facial recognition seems like an efficient practice of law enforcement, critics claim that artificial intelligence programs, like facial recognition, are "passive forms of investigation vastly expand[ing] policing power" under the 4th Amendment, as police are able to access bounties of information with just a click. However, other individuals like William Evans, Former Commissioner of the Boston Police Department, counter that facial recognition is only being used "to make our society safer" by recognizing people on most wanted lists or monitor schools and sports facilities.[28] Richland County Sheriff Leon Lott also claims that facial recognition is effective technology used solely as a "lead" in investigations.[29]

---

[25] *S.T.O.P. Condemns NYPD Facial Recognition Surveillance Of BLM Protest Leader*, S.T.O.P. (Aug. 14, 2020), https://www.stopspying.org/latest-news/2020/8/14/stop-condemns-nypd-facial-recognition-surveillance-of-blm-protest-leader.

[26] Steven Feldstein & David Wong, *New Technologies, New Problems—Troubling Surveillance Trends in America*, JUST SECURITY (Aug. 6, 2020), https://www.justsecurity.org/71837/new-technologies-new-problems-troubling-surveillance-trends-in-america/.

[27] FBI, *supra* note 10.

[28] *Three police chiefs discuss the future of facial recognition technology in law enforcement*, POLICE1 (Oct. 4, 2019), https://www.police1.com/police-products/police-technology/police-software/facial-recognition/videos/three-police-chiefs-discuss-the-future-of-facial-recognition-technology-in-law-enforcement-zU9V5i26x80ImvuA/.

[29] W. Thomas Smith Jr., *Facial recognition an effective investigative tool, not big brother*, POLICE1 (Aug. 13, 2020), https://www.police1.com/police-products/police-technology/police-software/facial-recognition/articles/facial-recognition-an-effective-investigative-tool-not-big-brother-XUjt1nBNz1SbVHJ5/.

Facial recognition works by identifying "more likely or less likely matches"[30] through the following process:

> [A]n algorithm must first find that person's face within the photo. This is called face detection. Once detected, a face is "normalized"—scaled, rotated, and aligned so that every face that the algorithm processes is in the same position. This makes it easier to compare the faces. Next, the algorithm extracts features from the face—characteristics that can be numerically quantified, like eye position or skin texture. Finally, the algorithm examines pairs of faces and issues a numerical score reflecting the similarity of their features.[31]

Through this process, facial recognition software can perform a variety of tasks. According to IBM, their technology is able to perform face detection, facial authentication, and facial matching.[32] Face detection identifies faces without attributing them to a particular individual, allowing for "count[ing] and analyz[ing] flows of people, bicycles, and cars" as well as "estimat[ing] the crowd size" at events.[33] Facial authentication uses "an individual's face for '1-to-1' authentication purposes" like unlocking a smartphone, while facial matching matches a face to a database of faces relying on "'1-to-many' matching."[34]

The FBI's NGI system, which includes a variety of tools including fingerprint, palm prints, and facial recognition databases and technology, was born out of the Integrated Automated Fingerprint Identification System created in 1999.[35] The FBI uses facial recognition in its investigations, while also allowing police to "submit a probe photo for a search against over 30 million criminal mug shot photos and receive a list of ranked candidates as potential investigative leads."[36] A potential problem with using mugshots is that the database is inherently biased, as black people are found to be "arrested at a rate five times higher than white people,"[37] leading to more

---

[30] Joseph N. Pato and Lynette I. Millett, eds., *Biometric Regonition: Challenges and Opportunities*, NAT'L ACAD. PRESS (2010).

[31] Claire Garavie, Alvaro Bedoyya & Jonathan Frankle, *Unregulated Police Face Recognition in America*, GEORGETOWN L. (October 18, 2016), https://www.perpetuallineup.org/background#footnote8_zix7uxb

[32] Christina Montgomery, Ryan Hagemann, *Precision Regulation and Facial Recognition*, IBM POLICY LAB, https://www.ibm.com/blogs/policy/wp-content/uploads/2019/11/IBM-Facial-Recognition-POV.pdf.

[33] *Id.*

[34] Montgomery & Hagemann, *supra* note 32.

[35] FBI, *supra* note 10.

[36] *Id.*

[37] Anagha Srikanth, *Black people 5 times more likely to be arrested than whites, according to new analysis*, THE HILL (June 11, 2020), https://thehill.com/changing-america/respect/equality/502277-black-people-5-times-more-likely-to-be-arrested-than-whites.

mugshots of black people than is proportionate to the total population. In addition to criminal mugshots, the FBI employs a database of driver's license photos provided by departments of motor vehicles in its facial recognition system.[38] This provides the FBI with all the information a driver's license contains including addresses, by requesting them from states' department of motor vehicles, who freely grants them the information.[39]

Outside of the FBI, police departments use a variety of facial recognition systems, including software from Amazon, Microsoft, and IBM.[40] Police also query "mugshot databases to identify people in photos taken from social media, CCTV, traffic cameras, or even photographs they've taken themselves in the field."[41] Amazon's Rekognition leaves it "up to the user to provide a 'face collection' that they own and manage" but it analyzes images and videos.[42] Presumably, police departments are using mugshots, traffic cameras, social media photos, and field photos to create their face collections. Microsoft's Face works similarly to Amazon's Rekognition by "match[ing] an individual in [a police department's] private repository of up to 1 million people."[43] IBM's Watson Visual Recognition works in a similar fashion, but can also "tag images for content, recognizes faces, and find similar faces" along with an option for the user to "train the Visual Recognition service to recognize specific content."[44]

In the summer of 2020, Amazon, Microsoft, and IBM all announced within a week of each other that they were halting sales of their facial recognition technology to law enforcement amidst police brutality protests.[45]

---

[38] Drew Harwell, FBI, *ICE find state driver's license photos are a gold mine for facial-recognition searches*, WASH. POST (July 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

[39] NAT'L IMMIGRATION LAW CENTER, *supra* note 8.

[40] Isobel Asher Hamilton, *Outrage over police brutality has finally convinced Amazon, Microsoft, and IBM to rule out selling facial recongition tech to law enforcement. Here's what's going on.*, BUS. INSIDER (June 13, 2020, 5:01 AM), https://www.businessinsider.com/amazon-microsoft-ibm-halt-selling-facial-recognition-to-police-2020-6.

[41] *Face Recognition: Street-Level Surveillance*, ELEC. FRONTIER FOUND. (Oct. 24, 2017), https://www.eff.org/pages/face-recognition#:~:text=Police%20collect%20mugshots%20from%20arrestees,police%20do%20another%20criminal%20search.

[42] Ry Crist, *Amazon's Rekognition software lets cops track faces: Here's what you need to know*, CNET (Mar. 19, 2019, 5:00 AM), https://www.cnet.com/news/what-is-amazon-rekognition-facial-recognition-software/.

[43] MICROSOFT AZURE, https://azure.microsoft.com/en-us/services/cognitive-services/face/, (last visited Oct. 23, 2020).

[44] Andrew Trice, *How to Sharpen Watson Visual Recognition Results with Simple Preprocessing*, IBM (March 17, 2017), https://www.ibm.com/cloud/blog/sharpen-watson-visual-recognition-results?mhsrc=ibmsearch_a&mhq=face%20recognition.

[45] Hamilton, *supra* note 40.

Amazon suspended its sales to law enforcement for one year calling for "stronger regulations to govern the ethical use of facial recognition technology."[46] IBM's CEO, Arvind Krishna stated, "IBM firmly opposes and will not condone uses of any technology, including facial recognition technology offered by other vendors, for mass surveillance, racial profiling, violations of basic human rights and freedoms" in an announcement letter to members of congress.[47] These halts were foreshadowed by concerned Amazon employees that advocated to Amazon's CEO, Jeff Bezos, to stop selling facial recognition to law enforcement and government agencies after "nearly 70 civil rights and research organizations wrote a letter to Jeff Bezos" calling for a stop in 2018 as the technology was enabling the tracking and deportation of immigrants.[48] Although major companies are withholding the technology until there is sufficient legal regulation, their efforts may not be as impactful as they hoped, since it has left the market open for other companies such as Clearview, Kairos, and PredPol to fill the gap without new, regulatory legislation.[49]

As of early 2021, there is little widespread legal regulation of facial recognition. Currently, local city councils in California has banned the use of facial recognition in law enforcement, [50] while lawmakers in Massachusetts passed a bill that bans facial recognition use in police departments and public agencies.[51] Similar to New Hampshire and Oregon, both which have laws prohibiting "facial recognition and biometric tracking technology in body cameras,"[52] California has recently enacted a more expansive bill that "prohibits a law enforcement agency or law enforcement officer from installing, activating, or using any biometric surveillance system in connection with an officer camera or data collected by an officer camera."[53] Although there are no national standards for the use of facial

[46] *Id.*

[47] Hamilton, *supra* note 40.

[48] Hao, *supra* note 20.

[49] Hamilton, *supra* note 40.

[50] Kaitlyn Burton, *SF Picks Side Of Privacy With Ban On Facial Recognition*, L. 360 (May 17, 2019, 9:50 PM EDT), https://www.law360.com/articles/1161059/sf-picks-side-of-privacy-with-ban-on-facial-recognition-tech.

[51] Taylor Hatmaker & Zack Whittaker, *Massachusetts lawmakers vote to pass a statewide police ban on facial recognition*, TECHCRUNCH (Dec. 1, 2020), https://techcrunch.com/2020/12/01/massachusetts-votes-to-pass-statewide-police-ban-on-facial-recognition/?guccounter=1.

[52] Susan Crawford, *Facial Recognition Laws Are (Literally) All Over the Map*, WIRED (Dec. 16, 2019 at 8:00 am), https://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/#:~:text=The%20current%20state%20of%20rules,literally%20all%20over%20the%20map.&text=In%20October%2C%20California%20joined%20New,tracking%20technology%20in%20body%20cameras.

[53] 2019 Bill Text CA A.B. 1215.

recognition in policing, Honorable Eddie Bernice Johnson of Texas proposed a bill to congress in 2020, The Promoting Fair and Effective Policing Through Research Act, remarking, "If we allow inaccuracies or biases to persist in these systems, then when deployed in high-impact situations, like decision making in the criminal justice system, those biases will disproportionately harm communities of color."[54] Another proposed bill, Stop Biometric Surveillance by Law Enforcement Act, introduced in 2020, advocates for prohibiting the use of facial recognition in police body cameras.[55] Currently the American Civil Liberties Union is suing the "FBI, DEA, ICE, and CBP" alleging they have "abused or even continue to abuse surveillance authority to spy on protesters, political opponent, Black and Brown communities, and more."[56] Overall, the absence of federal regulation of facial recognition laws vary greatly amongst the states absent federal regulation allowing states to act as the "testing grounds for new ideas."[57]

III. FACIAL RECOGNITION PROBLEMS

A. Racial Bias

Today, facial recognition technology is unreliable, as it mismatches minorities at a higher rate than white people.[58] For example, when the ACLU tested Amazon Rekognition, used by some police agencies, it disproportionally misidentified African-American and Latino individuals when the ACLU tested the technology by running federal lawmakers against a database of mugshots.[59] Additionally, a study from the National Institute of Standards and Technology found facial recognition's algorithm's "false positive rates are highest in West and East African and East Asian people, and lowest in Eastern European individuals."[60] Despite multiple findings that facial recognition technology is racially biased, law enforcement across America continues to use it.

One reason that the technology is racially biased is because of problems within the technology's algorithm. The algorithms can be racially biased as

---

[54] 166 Cong Rec. E 545.

[55] Stop Biometric Surveillance by Law Enforcement Act, 116 H.R. 7235.

[56] *The Fight to Stop Face Recognition Technology,* ACLU (July 15, 2021), https://www.aclu.org/news/topic/stopping-face-recognition-surveillance/.

[57] Crawford, *supra* notes 52.

[58] Harwell, *supra* note 16.

[59] Natasha Singer, *Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says*, N.Y. TIMES (July 26, 2018), https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html?login=facebook.

[60] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FACE RECOGNITIONN VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS (2009) https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

"some facial analysis algorithms misclassified Black women nearly 35 percent of the time, while nearly always getting it right for white men," and a federal study found "systems generally work best on middle-aged white men's faces, and not so well for people of color, women, children, or the elderly."[61] According to Joy Buolamwini, an MIT Media Lab researcher, one possible reason facial recognition is racially biased is because "its algorithms are usually written by white engineers who dominate the technology sector" who "build on pre-existing code libraries, typically written by other white engineers."[62] Essentially, a coder constructs the algorithms, but the coder will "focus on facial features that may be more visible in one race" which may also be influenced by the coder's "own experiences and understanding."[63] The algorithm that is produced is then geared toward white faces and is tested on mainly white subjects.[64] Further, although the software learns over time and becomes more accurate, the data sets composed of mostly white faces means that the "code 'learns' by looking at more white people – which doesn't help it improve with a diverse array of races."[65] This results in an algorithm that "misidentif[ies] dark-skinned people at a much higher rate than light-skinned people" because of the way it was trained;[66] hence, "algorithms trained with biased data have resulted in algorithmic discrimination."[67] Using biased algorithms results in facial recognition technology that misidentifies Asian and African American people "up to 100 times more likely" than white men.[68]

In addition to biased algorithms, there are also issues with the cameras that capture the images police use. For example, "[d]efault camera settings are often optimized to expose lighter skin better than darker skin" creating "underexposed or overexposed images," leading to "significant information loss" impacting accurate classification.[69] Testing this issue, one study,

---

[61] Kade Crockford, *How is Face Recognition Surveillance Technology Racist?*, ACLU (June 16, 2020), https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/.

[62] Ali Breland, *How White Engineers Built Racist Code— And Why It's Dangerous for Black People*, GUARDIAN (Dec. 4, 2017), https://www.theguardian.com/technology/2017/dec/04/racist-facial-recognition-white-coders-black-people-police.

[63] *Id.*

[64] *Id.*

[65] Breland, *supra* note 62.

[66] Haochen Sun, Article, *Reinvigorating the Human Right to Technology*, 41 Mich. J. Int'l L. 279.

[67] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, MIT MEDIA LAB, Feb. 4, 2018, https://www.media.mit.edu/publications/gender-shades-intersectional-accuracy-disparities-in-commercial-gender-classification/.

[68] Haochen Sun, Article, *The Fundamental Right to Technology*, 48 HOFSTRA L. REV. 445 (2020).

[69] Buolamwini et al., *supra* note 67.

conducted by Joy Buolamwini, a MIT researcher, and Timnit Gebru, a Microsoft researcher, measured the accuracy of three algorithms by comparing the algorithms' performance with pictures of people of various skin tones and genders.[70] The study found that "darker-skinned females are the most misclassified group (with error rates of up to 34.7%)" and the "maximum error rate for lighter-skinned males is 0.8%."[71]

Also of note are the databases that police use, since many facial recognition systems, like Amazon's Rekognition, work based on the police uploading their own database of images to compare with the image in question.[72] This is an issue, because "due to disproportionately high arrest rates, systems that rely on mug shot databases likely include a disproportionate number of African Americans."[73] This includes "countless individuals who have interacted with law enforcement" but were never actually convicted of a crime because they were found innocent or the charges were dropped.[74] Kade Crockford, Director of the ACLU of Massachusetts, warns that "using mugshot databases for face recognition recycles racial bias from the past, supercharging that bias with 21st century surveillance technology."[75]

Even though facial recognition systems include algorithms with coding issues and biased databases, police still use it to identify suspects, which begs the question of what happens when police wrongly identify someone like Robert Williams?[76] Although Williams had the resources to sue, there is little recourse outside of lodging complaints against police departments for these mistakes that take away the freedom of others.[77] In Williams's case, about 30 hours of his freedom away from his wife and daughters.[78] Citizens may bring an action for damages when they are wrongly arrested due to mistaken identity; however, to defend such a claim, an officer only has to show a good faith belief that the arrest warrant identified the subject even when the warrant was based on faulty facial recognition.[79]

---

[70] *Id.*

[71] *Id.*

[72] Crist, *supra* note 42.

[73] Garavie et al., *supra* notes 31.

[74] *Id.*

[75] Crockford, *supra* note 61.

[76] Williams, *supra* note 1.

[77] *Id.*

[78] *Id.*

[79] William v. Johnson, *Liability for false arrest or imprisonment under warrant as affected by mistake as to identity of person arrested*, 39 A.L.R. 4th 705.

B. Privacy Concerns

Law enforcement's use of facial recognition technology continues to erode the privacy of American citizens. The Fourth Amendment guarantees against unreasonable searches and seizures and the right of people to be secure in their persons, houses, papers, and effects.[80]Although the Supreme Court in *United States v. Carpenter* held that "technology-enhanced policing may trigger new Fourth Amendment protections," the Fourth Amendment has done little in terms of limiting the use of facial recognition.[81] If citizens attempt to bring a claim for a violation of the Fourth Amendment's protection against "unreasonable searches and seizures"[82] after facial recognition was used to identify them, the third-party doctrine will likely make that claim invalid.[83] The third-party doctrine makes the Fourth Amendment inapplicable if "information is 'voluntarily' conveyed to a third-party" rendering that "an individual has no reasonable expectation of privacy;" hence, when people are captured by a camera while in public they are voluntarily conveying that information to the system chosen by the law enforcement agency.[84] Even though there is little action a citizen can take to protect themselves in public against facial recognition, the technology has the power to reveal many details about them such as "[f]acial recognition-powered cameras in public squares" that can pull up a person's "citizenship, age, educational status, criminal history, employment, and even political affiliation…without their knowledge."[85] The police's use of facial recognition is expanding past just checking a security camera's footage against a database of mugshots, as some companies are already in the "development phase with a body camera that will include facial recognition software," despite warnings that continued expansion of the technology could create an overbearing government.[86] Such a government would continue to erode citizen's privacy protections under the Fourth Amendment.

Additionally, data privacy within these systems is of high concern. It is up to police departments to use their own discretion when choosing a facial recognition software meaning a variety of third party developers, including

---

[80] U.S. CONST. Amend. IV.

[81] Elizabeth E. Joh, Term, *Artificial Intelligence and Policing: Hints in the Carpenter Decision*, 16 OHIO ST. J. CRIM. L. 281.

[82] *Supra* note 80.

[83] Harvey Gee, *Last Call for the Third Party Doctrine in the Digital Age after Carpenter*, 26 B.U. J. SCI. & TECH. L. 286 (2020).

[84] Gee, *supra* note 83.

[85] Feldstein, *supra* note 26.

[86] Andrew Westrope, *Wolfcom Embraces Body Cam Face Recogntition Despite Concerns*, GOV'T TECH. (March 23, 2020), https://www.govtech.com/biz/Wolfcom-Embraces-Body-Cam-Face-Recognition-Despite-Concerns.html.

Amazon, IBM, and Microsoft, are being used.[87] In the summer of 2020 these three developers stopped selling their facial recognition software to law enforcement, but that creates room in the market for smaller companies like Clearview, Kairos, and PredPol to continue selling facial recognition software absent any laws prohibiting it.[88] Because of the absence of regulatory laws, these facial recognition software programs may be vulnerable to breaches by hackers. It is not known how or if companies are using the data that police input into the systems for other uses.

Further, in creating the databases for photographs to be compared to, systems are taking photographs from a variety of sources that a person may have never expected to be used for facial recognition purposes. For example, police departments can request to use the FBI's NGI,[89] but this too has been criticized.[90] NGI compares photographs to its database made up of "several different sources, including criminal mug shot photos, as well as photos from non-criminal sources such as employment records and background check databases."[91] NGI goes beyond using just criminal mugshots, since it uses photographs that were originally for non-criminal matters. It is argued that photos obtained from non-criminal sources such as pre-employment background checks, should "be used only as [the person] originally consented to . . . . rather than allowing the subsequent step of retaining photos and depositing them into the NGI along with criminal photos."[92] With little legal regulation, the FBI is able to pull from a variety of sources using data in a way that people never consented to.

A smaller company, Clearview AI, has provided its services "to hundreds of law enforcement agencies, ranging from local cops in Florida to the FBI and the Department of Homeland Security."[93] In November 2020, the Los Angeles Police Department halted all use of third party platforms after discovering that some detectives were using Clearview AI.[94] Clearview AI goes far beyond the bounds of where the FBI obtains its database of photos

[87] Hamilton, *supra* note 40.

[88] *Id.*

[89] Singer, *supra* note 59.

[90] Christopher De Lillo, *Open Face: Striking the Balance Between Privacy and Security with the FBI's Next Generation Identification System* 41 J. LEGIS. 264 (2015).

[91] De Lillo, *supra* note 90.

[92] *Id.*

[93] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[94] Richard Winton & Kevin Rector, *LAPD bars use of third-party facial recognition systems, launches review after BuzzFeed inquiry*, L.A. TIMES (Nov. 17, 2020), https://www.latimes.com/california/story/2020-11-17/lapd-bars-outside-facial-recognition-use-as-buzzfeed-inquiry-spurs-investigation.

as Clearview AI scrapes photographs from essentially any picture publicly posted on the internet at some point including on "Facebook, YouTube, Venmo and millions of other websites."[95] A reporter for the New York Times asked multiple police officers to run his photograph through Clearview AI's app to test its capabilities and the police officers began receiving "phone calls from company representatives asking if they were talking to the media — a sign that Clearview has the ability and, in this case, the appetite to monitor whom law enforcement is searching for,"[96] yet over 2,400 law enforcement agencies are using Clearview AI.[97] This presents a substantial risk, as "law enforcement agencies are uploading sensitive photos to the servers of a company whose ability to protect its data is untested," and, unregulated, given the gap in laws governing facial recognition use.[98] The ACLU is currently challenging the legality of Clearview AI's technology in an Illinois court after the company has "been secretly capturing untold numbers of biometric identifiers for purposes of surveillance and tracking, without notice to the individuals affected, much less their consent."[99] The issue is that police are using a variety of third parties for facial recognition use, but there is little known about how much access those companies continue to have to the data police input into the systems. This allows outsiders to peer into police investigations which are sensitive matters and elicits concerns about what the companies might do with the information. Third party insight into previously confidential police investigations can create distrust in the legal process as well as create opportunities for corruption if the companies sell the data.

Inquiring into the details of how a company uses the inputted data or how it works presents another barrier to transparency as "developers of data-driven systems are. . . .likely to depend more heavily on trade secret protections."[100] In a court setting, litigants are expected to be barred from inquiring into how technology operates, such as in *State v. Loomis*, the Wisconsin Supreme Court denied the defendant's claim to scrutinize trade secrets in an algorithm contained in the COMPAS risk assessment tool used at sentencing.[101] In the twenty-first century, an age of a dramatic increase in

95 Hill, *supra* note 93.

96 Hill, *supra* note 93.

97 Winton et al., *supra* note 94.

98 Hill, *supra* note 93.

99 ACLU, *supra* note 56.

100 Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018).

101 State v. Loomis, 2016 WI 68, 371 Wis. 2d 235, 881 N.W.2d 749.

the police's use of technology,[102] criminal cases are now invoking trade secret privilege that "states began to codify the trade secret privilege in the second half of the twentieth century."[103] By introducing trade secret privilege, traditionally asserted in civil cases to guard intellectual property interests, into criminal proceedings, defendants are experiencing increased barriers to their own access to evidence that could potentially take away their liberty.[104] Trade secret privilege doesn't preclude companies from being voluntarily transparent about their software, but technology created by private companies will likely always be at least partially shielded to create an advantageous business. In any case, trade secret privilege facilitates the lack of transparency in the technology. Trade secret privilege also creates significant burdens for plaintiffs, such as Robert Williams, to bring actions against law enforcement when they are wrongfully identified by facial recognition.[105]

When a party claims trade secret privilege, courts first "consider whether the alleged trade secret is valid," second, "they assess whether the information is relevant and necessary to the case," and third, "they weigh the risk of harm from disclosure against the need for the information."[106] Rebecca Wexler, a visiting fellow at Yale Law School, warns that claimants tend to overclaim trade secret privilege because criminal defendants are less "equipped with the resources to challenge the validity of an alleged trade secret" so claimants can expect their assertion will go unchallenged.[107] Another challenge for criminal defendants is that some courts "require[] showing that the information is needed to prove or rebut a theory at trial" in order to pass the necessity requirement.[108] Wexler criticizes that the third prong "place[s] pure financial interests on par with life and liberty."[109] Inquiring into the specifics of a facial recognition company's inner workings presents criminal defendants with significant barriers, although the company's technology may be used to take away their liberty.

The use of facial recognition technology in policing being largely unchecked poses a great threat of loss of privacy to society at large. The use

---

[102] *The Growing Role of Technology in the Criminal Justice Field*, PURDUE UNIV. GLOB. (April 9, 2018), https://www.purdueglobal.edu/blog/criminal-justice/growing-role-technology-criminal-justice/#:~:text=As%20technology%20is%20used%20to,%2C%20tracking%20systems%2C%20and%20more.

[103] Wexler, *supra* note 100.

[104] *Id.*

[105] Williams, *supra* note 1.

[106] Wexler, *supra* note 100.

[107] *Id.*

[108] *Id.*

[109] *Id.*

of facial recognition is expanding to create a society that is constantly surveilled, while third party companies are given unrestricted access into police investigations. This creates a need for laws to protect privacy and provide greater security to insure against these vulnerabilities, but until then, the scope and use of facial recognition technology is able to grow at quick rates.

C. Dilution of Democratic Participation

Police's use of facial recognition discourages democratic participation by increasing surveillance; even previously proposed legislation concerns use of facial recognition that would discourage free speech.[110] The ACLU warns that the use of facial recognition may lead "to a world where people are watched and identified as they attend a protest, congregate outside a place of worship, visit a medical provider, or simply go about their daily lives."[111] Over-expansive use of facial recognition technology may "open[] the door precisely to the cataloguing of individuals as they go about their daily lives" which is "fundamentally inconsistent with the values of democracy."[112]

A specific example of this concern is the use of facial recognition during protests, which only acts to intimidate protestors from exercising their First Amendment free speech right.[113] Robert Williams, in an article he wrote for the Washington Post, stated:

> Even if this technology does become accurate (at the expense of people like me), I don't want my daughters' faces to be part of some government database. I don't want cops showing up at their door because they were recorded at a protest the government didn't like. I don't want this technology automating and worsening the racist policies we're protesting. I don't want them to have a police record for something they didn't do — like I now do.[114]

Facially recognizing protestors has already begun. Organizations like S.T.O.P. have openly condemned the use of facial recognition by police after the NYPD used facial recognition to surveil a BLM protest leader in the summer of 2020.[115] Even the companies who are creating this facial

---

[110] Ethical Use of Facial Recognition Act, 116 S. 3284, 2020 S. 3284, 116 S. 3284.

[111] Neema Singh Guliani, *The FBI Has Access to over 640 Million Photos of Us Through Its Facial Recognition Database*, ACLU (June 7, 2019), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through.

[112] Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV 1591 (2017).

[113] U.S. CONST. Amend. I.

[114] Williams, *supra* note 1.

[115] S.T.O.P., *supra* note 25.

recognition technology understand the risks that it poses to democratic participation. After the protests surrounding racially inequalities began in June 2020 and more information about how facial recognition was contributing to racist policing surfaced, "IBM, Amazon, and Microsoft announced they would pause or end sales of their face recognition technology to police in the United States."[116] An Indiana district court stated that "[b]y prohibiting anonymity, it is a direct regulation of the content of speech or expression" when it affirmed the KKK's right to wear masks and prevent facial recognition during public assembly in *American KKK v. City of Goshen*.[117]

The use of facial recognition technology is expanding surveillance which has been used to stifle democratic participation in the past; thus, the abuse of surveillance that discourages democratic participation is not new. In the 1960s and 1970s, the FBI and National Security Agency "sp[ied] on civil rights leaders like Martin Luther King, Jr." which shows that "even well-established democracies [like the United States] struggle to maintain an appropriate balance between law enforcement imperatives, on the one hand, and citizens' rights on the other."[118] After September 9, 2001, the NYPD launched its Muslim Surveillance Program which sought to have an informant in every mosque within a 250-mile radius of New York City.[119] This widespread police surveillance was criticized for "chill[ing] some First Amendment-protected activities" as Muslim-Americans reported that they "avoided political demonstrations and gatherings, refrained from donating to potentially controversial charities or causes, avoided expressing political opinions, and altered their names or appearances" in response to the surveillance.[120] Facial recognition software goes beyond having an informant in a mosque, as facial recognition gives police the ability to instantly identify someone. The use of such powerful technology will stifle democratic participation in the population at-large, as the Muslim Surveillance Program did to Muslim-Americans. Increasing surveillance incentivizes individuals to permanently self-censor in order to avoid being detected, which "threatens the freedom of thought, belief, and speech that lie at the core of the liberties protected by the First Amendment."[121]

---

116 Crockford, *supra* note 61.

117 *Am. KKK v. City of Goshen*, 50 F. Supp. 2d 835 (N.D. Ind. 1999).

118 Feldstein, *supra* note 26.

119 Matthew A. Wasserman, *First Amendment Limitations on Police Surveillance: the Case of the Muslim Surveillance Program*, 90 N.Y.U. L. REV. 1786 (2015).

120 Wasserman, *supra* note 119.

121 *Id.*

Expanding the police's power to surveil communities with technology as powerful as facial recognition will result in individuals choosing not to protest, walk around their neighborhoods in fear of being surveilled by a digital camera[122], assemble at religious gatherings, or exercise other rights. If facial recognition is not limited in some way, this will create a society where individuals are constantly evaluating the risk of an activity for possibly being facially recognized. Unlike informant surveillance, facial recognition has the power to instantly pull up a person's "citizenship, age, educational status, criminal history, employment, and even political affiliation" making it far more powerful.[123]

IV. PROPOSED LIMITATIONS

A. Regulation Proposals in Criminal Proceedings

Since facial recognition is flawed by its inability to accurately provide matches by "misidentify[ing] black people, young people, and women at higher rates than[sic] white people, the elderly, and men," its admissibility in criminal proceedings must be limited and more transparent.[124] Even more concerning, facial recognition may be used to send someone to prison when it does not specify an exact match; instead, the results of a facial recognition query are rated likely or less likely matches.[125] Because of this ambiguity within facial recognition and racial bias, its use in the criminal process needs to be regulated.

The use of technology and biometrics to prove innocence or guilt is not new. DNA evidence is hailed as one of the most reliable biometric identifiers because of "its extraordinary specificity" in being able to "calculate that the probability of finding a random match between unrelated individuals" is "about 1 in 33 billion" in some cases.[126] Fingerprint evidence is even less reliable. The first case that used fingerprint evidence to convict was in 1906, and there are still doubts as to fingerprint evidence's reliability due to factors

[122] Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105 (2021).

[123] Feldstein, *supra* note 26.

[124] Karen Gullo & Jennifer Lynch, *When Facial Recognition is Used to Identify Defendants, They Have a right to Obtain Information About the Algorithms Used on Them, EFF Tells Court*, ELECTRONIC FRONTIER FOUNDATION (March 12, 2019), https://www.eff.org/deeplinks/2019/03/when-facial-recognition-used-identify-defendants-they-have-right-obtain.

[125] Gullo, supra note 124.

[126] Thomas M. Fleming, Annotation, *Admissibility of DNA Identification Evidence*, 84 A.L.R.4th 313.

such as doubting an expert's qualifications.[127] Even less reliable is the use of polygraphs, which are currently inadmissible in court. The Supreme Court held in *United States v. Scheffer* that polygraphs were inadmissible in court because they were unreliable and may bias the jury.[128]

On a spectrum of reliability, it is arguable that facial recognition falls more in line with polygraph evidence than DNA evidence. Polygraphs measure respiration, perspiration, and heart rate to monitor any spikes that may indicate a person is lying; however, they measure stress and not actual deception.[129] Because of this, psychologists and police officers claim it is "biased toward finding liars and has a 50 percent chance of hitting a false-positive for honest people."[130] Facial recognition has fundamental flaws that create unreliable outcomes analogous to polygraphs, and less like the scientific validity found in DNA evidence. The same logic in *United States v. Scheffer*, which rules polygraph evidence inadmissible in court, should be applied to facial recognition, as it has proven unreliable in mismatching racial minorities at a higher rate.[131] If the courts treat facial recognition evidence like a polygraph evidence, this decision will encourage police to continue to gather corroborating evidence and not tempt them to rely fully on facial recognition.[132] Until facial recognition's accuracy can be improved, it should also be open to debate like polygraphs as an MIT study found that people of color and women were "underrepresented in data used to train facial-recognition AI and assess its reliability."[133]

Another feature that may help to mitigate negative effects of facial recognition for defendants in trials is allowing defendants to inquire into the algorithm of the particular system, which would create more transparency in its use.[134] A possible route for allowing defendants to inquire more into facial recognition results would be through categorizing facial recognition results as *Brady* evidence.[135] The Supreme Court in *Brady v. Maryland* held "that suppression of evidence favorable to an accused upon request violated the

---

[127] Andre A. Moenssens, *Admissibility of Fingerprint Evidence and Constitutional Objections to Fingerprinting Raised in Criminal and Civil Cases*, 40 CHICAGO-KENT L.REV. 2 (1963).

[128] *U.S. v. Scheffer*, 523 U.S. 303 (1998).

[129] Adam James Levin-Areddy, *How Polygraphs Work—And Why They Aren't Admissible in Most Courts*, MENTAL FLOSS (Oct. 16, 2018), https://www.mentalfloss.com/article/560059/how-polygraphs-work-and-why-they-arent-admissible-court.

[130] *Id.*

[131] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *supra* note 60.

[132] Ovide, *supra* note 9.

[133] Sarah St. Vincent, *What if Police Use 'Rekognition' Without Telling Defendants?*, JUST SEC. (Aug. 6, 2020), https://www.justsecurity.org/57275/police-rekognition-telling-defendants/.

[134] Gullo, *supra* note 124.

[135] Andrew Guthrie Ferguson, *Big Data Prosecution and Brady*, 67 UCLA L. REV. 180 (2020).

Due Process Clause, U.S. Const. amend. XIV, where the evidence was material to guilt or punishment, regardless of the State's good or bad faith."[136] Facial recognition data should be disclosed to defendants under Brady, although it is not currently considered as *Brady* evidence.[137]

If a witness identifies multiple people as the potential suspect in a human line up, "the state would have had to disclose that information" to a defendant to allow the defendant to investigate alternative leads.[138] Similarly, facial recognition technology may identify multiple people as possible matches, but defendants are not always afforded the knowledge of who else the algorithm identified.[139] Big data, such as facial recognition, used in criminal prosecutions is engineered to favor the prosecution as it is not designed to "identify exculpatory or impeaching evidence for the defense,"[140] but evidence such as multiple facial recognition matches can imaginably be exculpatory or impeaching as it would identify other possible defendants. Concluding that multiple matches and other data produced by facial recognition software is *Brady* evidence, required to be turned over to the defense, is discretionary as the "favorable" and "materiality" requirements are often debated.[141] I argue that in relation to facial recognition, the results of a facial recognition software should always be regarded as *Brady* evidence as they provide an opportunity to explore other possible suspects, possibly exonerating the defendant. Under *Brady*, this type of evidence would be "material either to guilt or to punishment;"[142] thus, facial recognition results should be made available to defendants to promote fairness and transparency.

Treating facial recognition evidence as polygraph evidence, rendering it inadmissible at trial, or requiring the disclosure of facial recognition results under *Brady*, are two possibilities that would mitigate the risks of using biased technology. Preventing the admissibility of facial recognition evidence at trial would encourage police and prosecutors to do their due diligence in gathering other incriminating evidence to ensure the correct person is tried, while also preventing a jury from being unduly influenced. Characterizing it as *Brady* evidence would help to restore the balance of facial recognition evidence being heavily used as a tool for the prosecution by allowing a defendant to use it to help prove innocence. It would also

136 *Brady v. Maryland*, 373 U.S. 83 (1963).

137 *Id.*

138 Gullo, *supra* note 124.

139 *Id.*

140 Ferguson, *supra* note 135.

141 Ferguson, *supra* note 135.

142 *Brady*, 373 U.S.

promote transparency in how facial recognition is used if defendants have the right to inquire about its results. However, even with both of these suggestions, regulating facial recognition's use in criminal proceedings is just attempting to plug the holes of a sinking boat. It would be an attempt to restore some order of justice when people like Robert Williams are being wrongly arrested and held in prison after being facially recognized.[143] Creating new restrictions does not prevent these arrests or fix the algorithmic problems that lead to bias and mismatching.

B. Encourage a Singular Software for Use Amongst all Agencies

Police agencies are using a variety of facial recognition software which do not have many regulations. In addition to the erosion of everyday privacy due to the use of facial recognition, data privacy is of large concern. The potential that these third party companies have to do with the data inputted into the systems is largely unknown and unchecked. How the companies are obtaining photographs for databases may also constitute some ethical considerations. Due to trade secret privilege, inquiring into the specifics of a company's software would be difficult. Instead, I advocate that a single software system, like the FBI's NGI Facial Recognition, should be used amongst all agencies with the caveat being that the FBI can also claim trade secret privilege.

Requiring all agencies to adopt a uniform software system presents constitutional issues due to a 10th Amendment anti-commandeering violation, "refer[ring] to a federal requirement that state officials enact, administer, or enforce a federal regulatory program."[144] Congress could enact a law using its Spending Clause authority to give stipends to states to buy singular software as long as states' autonomy is preserved when bargaining with the federal government.[145] More probable is plainly giving the states a singular software in hopes that they will choose to use it in absence of individual state laws. Currently, the FBI already allows authorized law enforcement to submit a probe to its database.[146]

Encouraging law enforcement agencies to use a singular system presents a challenge, but will provide greater data protection if one system, monitored by the FBI, is used instead of countless third-party companies. An

---

143 Williams, *supra* note 1.

144 Neil S. Siegel, *Commandeering and Its Alternatives: A Federalism Perspective*, 59 VAND. L. REV. 1629 (2006).

145 Daniel S. Cohen, Article, *A Gun to Whose Head? Federalism, Localism, and the Spending Clause*, 123 DICK. L. REV. 421 (2019).

146 FBI, *supra* note 10.

inherent trust that the FBI is doing its due diligence in protecting data entered into the system is needed but trusting the FBI with data rather than a plethora of other companies or individual jurisdictions seems like a superior authority to trust. Afterall, this has worked in other ways as the FBI allows state law enforcement agencies to use its other biometric identification databases[147] which include the Combined DNA Index System (CODIS) and [148] Advanced Fingerprint Identification Technology (AFIT).[149] Additionally, if facial recognition software is used through the government, this eliminates the third-party doctrine concern that would negate any Fourth Amendment privacy claims, as the government is not considered a third-party under the Fourth Amendment.[150] Although the FBI already allows law enforcement agencies to use its facial recognition software, this must be more encouraged as agencies are actively using other companies.

In addition to being able to place greater trust in the FBI for data protection, the FBI has demonstrated a desire to improve algorithms as the FBI was able to improve the fingerprint matching algorithm in AFIT "from 92 percent to more than 99.6 percent."[151] Presuming the FBI would have the same desire to improve facial recognition's algorithm and accuracy, this would help to ensure that the facial recognition software law enforcement is using is being actively improved. The FBI's database may also be less biased as it uses mugshots[152] as well as driver license photos, so the database "primarily includes *law-abiding Americans*."[153] This helps the database itself to be less biased as only using mugshots means only using pictures of people who have been arrested. Having a larger database is significant because blacks have an arrest rate that is seven times higher than whites, meaning black people would be overrepresented in a mugshot-only database.[154] In the name of expediency and trust in the FBI to continually

147 *NGI Officially Replaces IAFIS—Yields More Search Options and Investigative Leads, and Increased Identification Accuracy*, FBI (Oct. 24, 2014), https://www.fbi.gov/services/cjis/cjis-link/ngi-officially-replaces-iafis-yields-more-search-options-and-investigative-leads-and-increased-identification-accuracy

148 *Frequently asked Questions on CODIS and NDIS*, FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (last visited Sept. 25, 2020).

149 FBI, *supra* note 10.

150 *See* discussion *supra* Part II.B.

151 FBI, *supra* note 10.

152 *Id.*

153 Clare Garvie, Alvaro Bedoya & Jonathan Frankle, Unregulated Police Face Recognition in America, THE PERPETUAL LINEUP (Oct. 18, 2016), https://www.perpetuallineup.org/.

154 Frank Shultz, *The race factor: Black arrest rate seven times higher than whites*, GAZETTEXTRA (February 10, 2019), https://www.gazettextra.com/news/crime/the-race-factor-black-arrest-rate-seven-times-higher-than-whites/article_389836cf-ab73-5589-93fd-674a89112933.html.

update their software due to political pressure, employing the FBI's facial recognition system across jurisdictions is better than individual jurisdictions creating their own facial recognition software.

Encouraging states to enact legislation that declares only the use of the FBI's NGI, or Congress using its Spending Clause power to encourage states to purchase one specific software would both help to mitigate some of the issues facial recognition technology presents. Namely, using one system instead of an innumerable number of different systems, would help to secure data security. This would still not provide much transparency due to trade secret privilege, but placing that burden of trust on one company or entity like the FBI would encourage the company to act ethically. If law enforcement agencies started solely using the FBI's NGI, trade secret privilege still would apply; however, the FBI already has incentives to continue to improve its algorithms across its biometric identification systems. The FBI already uses a database that is more representative of the population. Further, Kimberly J. Del Greco, Deputy Assistant Director of the Criminal Justice Information Services Division of the FBI gave a statement to the House Oversight and Reform Committee committing to the transparency in FBI's use facial recognition use in government including limiting "which facial recognition tools may be utilized" and committing "to ensuring that FBI facial recognition capabilities are regularly tested, evaluated, and improved."[155] The FBI is already striving to achieve strict self-proclaimed standards for its facial recognition software, which cannot be ensured across all facial recognition companies. Conversely, even if states were to adopt the use of one system, this would not solve other issues with facial recognition as the technology is currently inaccurate across various databases. Another uphill battle to encourage states to use one software is congress's inability to expressly mandate a singular software due to constitutional laws; hence, achieving one software being used across all agencies is unlikely.

C. Ban the Use of Facial Recognition in Body Cameras

In an attempt to avoid an Orwellian society in which citizens' daily lives are closely monitored by facial recognition, and Fourth Amendment privacy protections are basically nonexistent, I propose that the use of facial recognition technology be heavily regulated by banning real time facial recognition. Today, facial recognition is widely used to compare a photograph from a surveillance camera against a database of photographs to find likely matches, but it could also be used to monitor society in real time

[155] Kimberly J. Del Greco, *Facial Recognition Technology: Ensuring Transparency in Government Use*, FBI (June 4, 2019), https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use.

by being placed in street cameras or body cameras. The Metropolitan Police in London have started to use facial recognition in street cameras, which some have already called a "serious threat to civil liberties."[156] Because facial recognition in body cameras is a reality in the United States, California has banned its use in body cameras to prevent "body cameras from 'being transformed into roving surveillance devices that track our faces, voices, and even the unique way we walk.'"[157] Body cameras were originally implemented for police accountability, but now they have the ability to be a sword for the police.[158] Banning real time facial recognition in policing would help prevent discouraging democratic participation as people would become fearful of being identified during everyday activities if used.

In an interview with Montel Williams about Coresight, a company with an Israel-based facial recognition technology branch, he advocated for the use of real time facial recognition in policing.[159] One of his main arguments was that real time facial recognition would contribute positively to the world in scenarios such as identifying sexual predators through street cameras around schools.[160] While real-time facial recognition would have the ability to prevent egregious crimes, when weighed against the negative impacts, its advantages are small. According to Williams, Coresight's facial recognition only stores a picture of an individual when it identifies a positive match to a targeted suspect;[161] however, this does not close the door to other companies expansively tracking individuals. It does show the ability for companies to limit their reach into the data that is created using facial recognition software.

Police's scope of surveillance needs to be tightened in order to prevent more instances similar to the NYPD's Muslim Surveillance Program, where the police decided that a "religious belief and practice[]s [is] a basis for law enforcement scrutiny."[162] The use of surveillance technology in policing has "dramatically expanded" after the implementation of "automatic license plate

---

156 Vikram Dodd, *Met police to being using live facial recognition cameras in London*, THE GUARDIAN (Jan. 24, 2020), https://www.theguardian.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras.

157 Sidney Fussell, *Did Body Cameras Backfire?*, THE ATLANTIC (Nov. 1, 2019), https://www.theatlantic.com/technology/archive/2019/11/border-patrol-weighs-body-cameras-face-recognition/600469/.

158 Matt Cagle, *California Just Blocked Police Body Cam Use of Face Recognition*, ACLU (Oct. 11, 2019 at 11:45 AM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/california-just-blocked-police-body-cam-use-face.

159 Telephone Interview with Montel Williams, Coresight, (November 3, 2020).

160 *Id.*

161 *Id.*

162 *Factsheet: The NYPD Muslim Surveillance Program*, ACLU, https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program (last visited Nov. 10, 2021).

readers (ALPR), surveillance cameras, red light cameras, speed cameras, and biometric technology like facial recognition."[163] These technologies "only collect information on public movements and behaviors" which "prevents privacy concerns" for communities.[164] Although facial recognition is only one surveillance technology, it is one of the most powerful. In order to prevent it being used to track everyday movements, its use in policing needs to be limited in scope.

Grumblings of legislation preventing real time facial recognition are beginning to occur as one currently proposed bill "[p]rohibits a law enforcement officer or agency from installing, activating, or using a biometric surveillance system in connection with a law enforcement agency's body-worn camera or any other camera."[165] Additionally, California has provided a precedent blocking the use of facial recognition in body cameras to prevent body cameras from being used for community surveillance instead of police accountability.[166] Congress must enact legislation that would prevent real time facial recognition before it is widely implemented and used in order to protect the privacy of people's everyday lives. Limiting its use in real time is a preventative measure to expansive police power, but it does not solve the problems that are present in facial recognition which is not being used in a real time context.

V. CONCLUSION

While law enforcement's relatively new use of facial recognition as technology expands, a new gap in legal regulation has been created. So far, the technology has proven to have a racial bias along with eroding privacy and stifling democratic participation. Police recognize these deficiencies as their efforts "suggest that we are moving toward more efforts to improve the technology;" however, they are not "surrendering to the idea that the technology may not yet be sufficiently supplicated and should be shelved until such time."[167] Facial recognition technology may be limited in several ways including restrictions on its use in criminal proceedings, encouraging a singular software to be used amongst agencies, and prohibiting real time facial recognition, but until the technology is limited in scope and inaccuracies are minimized, it needs to be banned within policing. At least

163 Steven Rushin, *The Legislative Response to Mass Police Surveillance*, 79 BROOK. L. REV. 1 (2013).

164 *Id.*

165 2019 Legis. Bill Hist. CA A.B. 1215.

166 Matt Cagle, *California Just Blocked Police Body Cam Use of Face Recognition*, ACLU (Oct. 11, 2019 at 11:45 AM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/california-just-blocked-police-body-cam-use-face.

167 Nakar, *supra* note 13.

three cities, including San Francisco, Somerville, Massachusetts, and Oakland, California, have banned law enforcement's use of facial recognition already,[168] while Massachusetts recently banned facial recognition use across the state.[169] The rest of the United States should follow suit in order to prevent people like Robert Williams from being subject to its unfair use that takes away their liberties.[170]

[168] Gaffary, *supra* note 11.

[169] Hatmaker & Whittaker, *supra* note 51.

[170] Williams, *supra* note 1.