American University International Law Review

Volume 39 | Issue 3 Article 3

2024

Law Enforcement Use of Facial Recognition - A Comparative Approach Between the United States and Europe to Tackle the Racial Bias of Facial Recognition Against People of Color

Louise Grégoire
lgregoire@umaryland.edu

Recommended Citation

Grégoire, Louise (2024) "Law Enforcement Use of Facial Recognition - A Comparative Approach Between the United States and Europe to Tackle the Racial Bias of Facial Recognition Against People of Color," *American University International Law Review*: Vol. 39: Iss. 3, Article 3.
Available at: https://digitalcommons.wcl.american.edu/auilr/vol39/iss3/3

LAW ENFORCEMENT USE OF FACIAL RECOGNITION—A COMPARATIVE APPROACH BETWEEN THE UNITED STATES AND EUROPE TO TACKLE THE RACIAL BIAS OF FACIAL RECOGNITION AGAINST PEOPLE OF COLOR

LOUISE GRÉGOIRE*

* Ms. Grégoire is a LL.M. graduate from the University of Maryland, Francis King Carey School of Law. She also earned a Master's degree in English and North American Business Law from the University Paris 1 Pantheon – La Sorbonne and a Master's degree and Bachelor's degree from the University of Tours.

I. INTRODUCTION

In a dystopian world, George Orwell described Oceania's citizens' lives under a totalitarian regime where citizens are under surveillance by the regime in place 24/7 and human rights are restricted, and even nonexistent.[1] Although such regimes were originally based on fictional worlds, what the author described in 1949 has become reality.[2] Technology has become extremely present in our daily lives, being an efficient tool for governments and law enforcement to monitor crowds and determine whether an individual is a potential suspect that the police are looking for.

Facial recognition technology (FRT) symbolizes the development of technology in our society.[3] FRT might seem overly intrusive, but it may benefit public safety, identification, and arrest of criminal suspects.[4] Since the twenty-first century, FRT has been heavily used by law enforcement.[5] Despite its benefits, this technology raises

[1] *See* Cathy Lowne, *Nineteen Eighty-four*, ENCYCLOPEDIA BRITTANICA (Jan. 4, 2024), https://www.britannica.com/topic/Nineteen-Eighty-four (describing Orwell's book theme of totalitarianism and its manifestation through "Thought Police" and constant surveillance).

[2] *See* Jean Seaton, *Why Orwell's 1984 Could Be About Now*, BBC (Feb. 24, 2022), https://www.bbc.com/culture/article/20180507-why-orwells-1984-could-be-about-now (arguing Orwell's book, 1984, is ever relevant today in a state of constant surveillance).

[3] *See* Ashley Del Villar & Myaisha Hayes, *How Face Recognition Fuels Racist Systems of Policing and Immigration — And Why Congress Must Act Now*, ACLU (July 22, 2021), https://www.aclu.org/news/privacy-technology/how-face-recognition-fuels-racist-systems-of-policing-and-immigration-and-why-congress-must-act-now (explaining that society uses facial recognition technology and other biometric surveillance almost daily).

[4] *See The Man in the Hat Identified Thanks to FBI Software*, THE BRUSSELS TIMES (Apr. 14, 2016), https://www.brusselstimes.com/37264/the-man-in-the-hat-identified-thanks-to-fbi-software (exemplifying beneficial use of facial recognition for police work and identifying suspects).

[5] *See Facial Recognition Tech., Fed. Law Enf't Agencies Should Have Better Awareness of Sys. Used By Emp. GAO-21-105309: Testimony Before the S. Comm. on Crime, Terrorism and Homeland Sec.*, 117th Cong. (2021) (statement of Gretta L. Goodwin, Dir., Homeland Sec. and Just., U.S. Gov't Accountability Off.) (pointing out that twenty out of forty-two federal agencies surveyed employ law enforcement entities and officers that use facial recognition technologies for criminal investigations).

several disturbing issues, especially regarding its inaccuracy. FRT is known for misidentifying people, especially people of color.[6] In November 2022, a Black man from Georgia, Randall Reid, was arrested for stealing high-end Chanel and Louis Vuitton bags and was locked up for nearly a year.[7] Despite Reid never having been to Louisiana, where the incident occurred, facial recognition misidentified Reid as the suspect.[8] Unfortunately over the years, there have been similar stories of FRT's misidentification of Black people. As law enforcement has been denounced for racism against people of color in Europe and the United States, the continued use of FRT will likely further perpetuate racial biases.[9]

This article will focus on the use of FRT by law enforcement in the United States and in Europe and the racial biases involved in the use of the technology. Part II will focus on how bias originates from codes and datasets and how the inaccuracy of facial recognition disproportionately affects people of color and reinforces discrimination. Part III will discuss the implications on human rights and how the rights of people of color are especially targeted. Part IV will examine the current regulations and frameworks at the national and regional levels to tackle discrimination and highlight their insufficiencies in tackling the impact of these technologies on people of color. Finally, Part V will propose the legal possibilities for state institutions to better limit the racial bias of facial recognition.

[6] *See* 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 (indicating the technology has a tendency to be racially biased when coupled with the use of mugshot databases, since people of color face arrest at higher rates).

[7] *See* Kashmir Hill & Ryan Mac, *'Thousands of Dollars for Something I Didn't Do,'* N.Y. TIMES (Mar. 31, 2023), https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html (reporting on the erroneous facial recognition of Randal Quarn Reid in 2023 which led to his wrongful arrest and six days in jail).

[8] *See id.* (explaining the crime was committed in Louisiana, a state Mr. Reid had never been to and was the result of bad facial recognition).

[9] *See* Villar & Hayes, *supra* note 3 (indicating FRT will only continue to perpetuate and exacerbate state sanctioned violence against people of color).

II. FACIAL RECOGNITION USE BY LAW ENFORCEMENT AND ITS THREAT TO PEOPLE OF COLOR

Facial recognition technology (FRT) is being increasingly used across law enforcement departments in Europe and the United States.[10] In the United States between 2018 and 2020, more than 1800 police agencies used FRT,[11] and federal agencies such as the Federal Bureau of Investigation (FBI)[12] and Immigration and Customs Enforcement (ICE)[13] heavily relied on it. In Europe, FRT has been used for border control despite the harmful consequences that might occur as a result.[14] FRT will also potentially be used to monitor the 2024 Olympic Games in Paris,[15] despite its proven inaccuracy that

[10] *See* Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html (reporting that police departments in New York, Los Angeles, Chicago, Florida, and other federal agencies use FRT for daily policing); *see also* Gian Volpicelli, *EU Set to Allow Draconian Use of Facial Recognition Tech, Say Lawmakers*, POLITICO (Jan. 16, 2024, 2:28 PM), https://www.politico.eu/article/eu-ai-facial-recognition-tech-act-late-tweaks-attack-civil-rights-key-lawmaker-hahn-warns (allowing the use of facial recognition for law enforcement purposes in Europe after passage of the European Union Artificial Intelligence Act).

[11] *See* Andrea Cipriano, *Facial Recognition Now Used in Over 1,800 Police Agencies: Report*, THE CRIME REPORT (Apr. 7, 2021), https://thecrimereport.org/2021/04/07/facial-recognition-now-used-in-over-1800-police-agencies-report (noting the number of individual searches is around 340,000 across 1,803 public agencies between 2018 and 2020).

[12] *See Facial Recognition Technology: Part II Ensuring Transparency in Government Use: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. 4 (2019) (statement of Kimberly J. Del Greco, Deputy Assistant Dir., Crim. Just. Info. Serv. Div., FBI) [hereinafter *Del Greco Statement*] (stating the two systems used by the FBI are the Interstate Photo System and the Facial Analysis Comparison and Evaluation).

[13] *See* Drew Harwell & Erin Cox, *ICE Has Run Facial Recognition Searches on Millions of Maryland Drivers*, WASH. POST (Feb. 26, 2020, 10:55 PM), https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers (allowing ICE officials to conduct facial recognition searches on Maryland license photos without having to first seek state or court approval).

[14] *See* Costica Dumbrava, European Parliamentary Research Service (EPRS), *Artificial Intelligence at EU Borders,* 5–6, 27 (2021) (reporting facial recognition is less accurate for women and people of color).

[15] *See* Louis Neveu, *La France mise sur des caméras intelligentes pour la*

disproportionately impacts people of color.

A. RACIAL BIAS WITHIN THE TECHNOLOGY

FRT is the automatic treatment of digital images that "contains an individual's face to identify, verify or authenticate a person or a group of people."[16] This biometric method operates in several steps. First, the technology must collect an image of a face from either a video or a picture to generate a sample that will contain the specific characteristics of the face in the captured image.[17] Second, the sample is compared to a sample contained in a database to identify or control a person's identity. FRT is more intrusive than video protection and video surveillance since those technologies do not associate an image or a face with an identity.[18] However, FRT can be integrated into these existing technologies.[19]

FRT can have different purposes. For example, FRT might be used for a "one-to-one match" authentication purpose by comparing two images to determine if the person in the picture is the same one.[20] This

sécurité des Jeux Olympiques, FUTURA (Jan. 24, 2023), https://www.futura-sciences.com/tech/actualites/technologie-france-mise-cameras-intelligentes-securite-jeux-olympiques-paris-103019 (reporting that the French government has authorized the use of FRT and other video surveillance for safety during the 2024 Olympics).

[16] *See Article 29 Data Protection Working Party of the European Commission Opinion 02/2012 on Facial Recognition in Online and Mobile Services*, at 2 (March 22, 2012).

[17] *See Reconnaissance faciale [Facial recognition]*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (CNIL) https://www.cnil.fr/fr/definition/reconnaissance-faciale (Fr.) (stating the data collected from an image is biometric data withing the meaning of Article 4-14 of the General Data Protection Regulation of the European Union).

[18] *See Vidéoprotection: quelles sont les dispositions applicables ? [Video protection: what are the applicable provisions?]*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (CNIL) (Dec. 13, 2019), https://www.cnil.fr/fr/videoprotection-quelles-sont-les-dispositions-applicables (Fr.) (describing video production and surveillance as "classic").

[19] *See Reconnaissance faciale: pour un débat à la hauteur des enjeux [Facial recognition: for a debate at the height of the stakes]*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL) (Nov. 14, 2019), https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux (Fr) (explaining facial recognition should not be confused with other image processing, although sometimes the two are combined).

[20] *Facial Recognition*, *supra* note 17.

process is mostly used by government agencies at airports, ports, or train stations.[21] Second, FRT might be used for identification or "one-to-many" research.[22] Under this process, FRT will compare a given template to several pictures stocked in a database to identify the person captured in the template.[23] When FRT is deployed in real-time, a face can be spotted in a live crowd of people. Police officers might use FRT to narrow their list of persons of interest. Additionally, some companies and federal agencies might use facial recognition software for categorization purposes. Contrary to identification and verification, categorization is not used to recognize and identify an individual.[24] FRT extracts information on an individual's characteristics, which permits the labeling of people on the grounds of their race, age, and gender.[25]

Depending on how the program is designed, an FRT algorithm might provide a range of possible matches or one match with some kind of measurement of the algorithm's confidence that the person has been correctly identified. FRT software relies on different algorithms with a distinct level of accuracy. The accuracy rate of FRT is largely impacted by the diversity of its databases and the physical conditions in which FRT is deployed; for instance, in 2014 the National Institute of Standards and Technology (NIST) found that the best facial

[21] *See TSA PreCheck®: Touchless Identity Solution*, TSA, https://www.tsa.gov/biometrics-technology/evaluating-facial-identification-technology (explaining the U.S. Transportation Security Administration's (TSA) use of facial identification at security checkpoints, especially for TSA PreCheck at airports).

[22] *About Face: Examining The Dep't of Homeland Security's Use Of Facial Recognition And Other Biometric Tech., Part II: Hearing Before H. Comm. on Homeland Security*, 116th Cong. (2020) (statement of Charles H. Romine, Dir., Info. Tch. Lab. Nat. Inst. of Standards & Tech., U.S. Dep't of Commerce) [hereinafter Romine Statement Feb. 2020].

[23] *See id.* (explaining the difference between "one-to-one" matching and "one-to-many" matching in face detection technology: "one-to-one" *verifies* that a person pictured is the person pictured whereas "one-to-many" *identifies* the person pictured).

[24] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-20-552, FACIAL RECOGNITION TECH.: PRIV. & ACCURACY RELATED TO COM. USES, 7 (July 2020) ("Facial analysis—sometimes also referred to as facial classification or characterization—is a technology distinct from facial recognition. Whereas facial recognition matches a face to a specific identify, facial analysis uses a facial image to estimate or classify personal characteristics such as age, race, or gender.").

[25] *Id.*

recognition system has an error rate of 4.1%, but in 2020 the same software had an error rate of only 0.08%.[26] If these results show a high accuracy of FRT, these results are highly circumstantial. Indeed, the NIST's Facial Recognition Vendor Test (FRTV) found that the error rate for high-quality mugshots is 0.1%; however, this rate rose to 9.3% for pictures of average quality.[27] Studies have found that the accuracy of FRT results depends on the quality and precision of the pictures and data.[28] The inaccuracy of facial recognition has been emphasized by the surveys released by law enforcement agencies. In June 2020, the Detroit Police Chief admitted that the software they use misidentified people 96% of the time.[29] Similarly, the South Wales police department has said that its software misrecognizes people 98% of the time.[30] It might be noted that these numbers consider people from all races. While inaccuracy according to these numbers affects all people, the rate of inaccuracy is higher for people of color.

Several studies have demonstrated the inaccuracy of facial recognition technology for ethnic minorities, especially the African American population. In 2018, Joy Buolamwini and Timnit Gebru researched that the maximum error rate for white men was 0.8% whereas the error rate for darker-skin women was 34.7%.[31] In 2019,

[26] William Crumpler, *How Accurate Are Facial Recognition Systems – and Why Does It Matter?*, CTR. FOR STRATEGIC & INT'L STUD.: BLOG POST (Apr. 14, 2020), https://www.csis.org/blogs/strategic-technologies-blog/how-accurate-are-facial-recognition-systems-and-why-does-it.

[27] *See id.* (indicating higher accuracy is only present in clear photos and videos with consistent lighting and positioning).

[28] *See* European Union Agency for Fundamental Rights (FRA), *Facial Recognition Technology: Fundamental Rights Consideration in the Context of Law Enforcement* 10 (2020) (noting the factors that influence the quality of facial images and likelihood of accurate conclusions includes backgrounds, illumination, light reflections, ergonomics, age, gender, skin color, and skin conditions).

[29] Jason Koebler, *Detroit Police Chief: Facial Recognition Misidentified 96% of the Time*, VICE (June 29, 2020, 12:56 PM), https://www.vice.com/en/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time.

[30] Jon Sharman, *Metropolitan Police's Facial Recognition Technology 98% Inaccurate, Figures Show*, INDEPENDENT (May 13, 2019, 1:07 PM), https://www.independent.co.uk/news/uk/home-news/met-police-facial-recognition-success-south-wales-trial-home-office-false-positive-a8345036.html.

[31] *See* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 1, 9 (2018) (showing statistics for facial recognition inaccuracies

the NIST tested 189 software from 99 different organizations. It found that FRT resulted in more discrimination against African Americans, especially women, elderly people, and children because of the higher likelihood of them being misidentified by the technology.[32] In 2018, the American Civil Liberties Union (ACLU) found that Amazon's software Rekognition, which is used by law enforcement in the United States, misidentified 28 members of the U.S. Congress with available mugshots.[33] Among these twenty-eight misidentified individuals, 40% were African American.[34] However, only 20% of the U.S. Congress is African American, therefore the software disproportionally misidentified people of color.[35] These studies outlined the high level of inaccuracy regarding African Americans, leading to misidentified Black people and harmful consequences.

In Europe, facial recognition used at country borders also showed significant inaccuracies. The European Fundamental Rights Agency (FRA) surveyed the staff at the border crossing points and at the Diplomatic Missions and Consular Posts (DMCP). They were asked how often they or their colleagues found that some of the personal data—such as name, sex, nationality, or age—inserted in the Visa Information System (VIS) or Schengen Information System (SIS II) are inaccurate, incorrect, or not updated.[36] For SIS II, more than 40% of the DMCP staff indicated that incidents of wrong matches or inaccurate data sometimes occur in these databases.[37] For VIS, it was

across race and gender).

[32] *See* 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 PM), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition (indicating African Americans were 100 times more likely to be misidentified compared to white men and women more likely to be falsely identified compared to men).

[33] *See* Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (July 26, 2018), https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28 (indicating misidentification can happen across race, gender, age, and political affiliation).

[34] *See id.* (noting that although the software misidentified people of all races, the software still disproportionally resulted in false matches for people of color).

[35] *Id.*

[36] *See* European Union Agency for Fundamental Rights (FRA), *Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights* 82 (2018) (reporting on gaps and inaccuracies at European border crossings).

[37] *Id.*

slightly more than 50%.[38] Migrants and people from ethnic minorities are therefore more likely to be misidentified. Similar to the United States, FRT suffers from significant bias against people of color in Europe.

These results are explained by the design and data of the software. Facial recognition identifies individuals and learns what a face is supposed to look like by training on a dataset. The dataset needs to be diverse enough to correctly interpret a face.[39] If the database is tested or is based on the photographs of faces of one skin color, the test will not reflect how well the FRT will perform on faces that do not share that skin color.[40] The design of the software and databases introduce biases within the technology. Engineers are generally white males and may favor their own characteristics, otherwise known as the "own-race effect."[41] Under the own-race effect, people can better identify people from their own race and therefore favor their own characteristics.[42] The theory further implies that white male engineers when drafting codes may favor white men's characteristics.[43] This would result in the creation of a system that might be accurate for white men but misrepresents black men. Indeed, a biased test leads to biased results. Unfortunately, police might not correct these biases, which in turn reinforces the existing racism among law enforcement.

[38] *Id.*

[39] *See Facial Recognition Tech. (Part III): Ensuring Com. Transparency & Accuracy: Hearing Before H. Comm. on Oversight and Gov't Reform*, 116th Cong. 7 (2020) (statement of Brenda Leong, Senior Couns. and Dir. of AI and Ethics Future of Priv. F.) [hereinafter Leong Statement Jan. 2020] (arguing that technologies and their quality varied widely partly based on available databases).

[40] Lindsey Barret, *Ban Facial Recognition Technologies For Children – And For Everyone Else*, 26 B.U.J. SCI. & TECH. L. 223, 230–32 (2022).

[41] *See* Queenie Wong, *Why Facial Recognition's Racial Bias Problem Is So Hard to Crack*, CNET (Mar. 27, 2019, 5:00 AM), https://www.cnet.com/news/why-facial-recognitions-racial-bias-problem-is-so-hard-to-crack ("Engineers at tech companies, which are made up of mostly white men, might also be unwittingly designing the facial recognition systems to work better at identifying certain races. . . .").

[42] James W. Tanaka et al., *A Holistic Account of The Own-Race Effect in Facial Recognition: Evidence From a Cross-Cultural Study*, 93 COGNITION, B1, B2 (2004).

[43] *See* Wong, *supra* note 41.

B. THE REINFORCEMENT OF RACIAL BIAS WITHIN LAW ENFORCEMENT

Law enforcement has been criticized for discriminatory behaviors in the United States for decades. For example, "[d]uring the nearly 100 years of Jim Crow segregation, police officers were known to take off their uniforms in the evening and replace them with their Klan robes, contributing to the lynching of thousands of Black people with impunity."[44] Despite the abolishment of Jim Crow laws, people of color are still disproportionately arrested by the police today.[45] In 2018, Black people were arrested five times more than White people in the United States.[46]

Further, U.S. laws tend to lead to higher criminalization of Black people than White people. For instance, while the same proportion of White and Black people consume marijuana, Black people tend to be arrested more often than White people on marijuana charges.[47] Each time someone is arrested, police take a mug shot and store the picture in a database.[48] However, because law enforcement disproportionately targets communities of color, law enforcement further targets Black people disproportionately by using its mugshot databases to identify

[44] Cloee Cooper, *The Racist History of U.S. Law Enforcement*, THE PROGRESSIVE MAG. (Feb. 22, 2021, 8:00 AM), https://progressive.org/latest/racist-history-law-enforcement-cooper-210222.

[45] *See id.* (detailing how in the past few decades law enforcement and anti-terrorism legislation has disproportionately targeted communities of color).

[46] Pierre Thomas, et al., *ABC News Analysis of Police Arrests Nationwide Reveals Stark Racial Disparity*, ABC NEWS (June 11, 2020, 5:04 AM), https://abcnews.go.com/US/abc-news-analysis-police-arrests-nationwide-reveals-stark/story?id=71188546.

[47] Karine Elwood & John D. Harden, *After Virginia Legalized Pot, Majority of Defendants are Still Black*, WASH. POST (Oct. 16, 2022, 7:00 AM), https://www.washingtonpost.com/dc-md-va/2022/10/16/virginia-marijuana-enforcement-disparities; Fred Dews, *Charts of the Week: Marijuana Use by Race, Islamist Rule in the Middle East, Climate Adaptation Savings*, BROOKINGS INST. (Aug. 11, 2017), https://www.brookings.edu/articles/charts-of-the-week-marijuana-use-by-race.

[48] *See* Joseph Scanlon, *Face It: Police Can't Be Trusted with Facial Recognition Technology*, MINNESOTA J.L. & INEQ.: INEQ. INQUIRY BLOG (Mar. 7, 2023), https://lawandinequality.org/2023/03/07/face-it-police-cant-be-trusted-with-facial-recognition-technology/ ("In turn, mugshot photos are used to feed facial recognition databases and subsequently identify suspects of more serious crimes. More egregiously, some cities disproportionately implement facial recognition technology in majority-Black areas, leading to even more misidentifications.").

suspects with racially biased FRT. Thus, Black people are more susceptible to being misidentified and wrongfully arrested.

For instance, in 2020, Robert Julian-Borchak Williams was arrested by the Detroit Police Department for "felony warrant" and "larceny."[49] The police detained and took Mr. Williams's mug shot, fingerprints, and DNA. During his interrogation, the police showed an image of the robbery to Mr. Williams which indicated that he was the individual in the image. Relying on Mr. Williams's old mug shot, the software identified Mr. Williams without verification protocols. As a result, Mr. Williams was misidentified by the facial recognition of the Detroit Police.[50] This case illustrates that the disproportion of mugshots might disfavor African Americans.[51]

Facial recognition might also reinforce racial biases in law enforcement. Researchers have proven that law enforcement, specifically in the U.S., tends to target Black communities.[52] Additionally, it has been proven that there are racial disparities in police practices, such as deceptive and coercive interrogation techniques toward young black teenagers.[53] Black people receive dissimilar treatment and FRT will deepen this conclusion. By using FRT, police officers might think that their decision is sound and legitimate because the technology identified the person. Thus, like in the incident with Mr. Williams, law enforcement might not verify and double-check the findings of the technology. Once a Black person is identified, the police might rely on the finding without any verification and wrongfully arrest the individual. If the Police are questioned about the misidentification, they may blame FRT's inaccuracies without

[49] Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

[50] *Id.*

[51] *Id.*

[52] *See* Leona D. Jochnowitz & Tonya Kendall, *Analyzing Wrongful Convictions Beyond the Traditional Canonical List of Errors, for Enduring Structural and Sociological Attributes, (Juveniles, Racism, Adversary System, Policing Policies)*, 37 TOURO L. REV. 579, 588–90 (explaining the role of stereotypes in the racial disparities of law enforcement, especially with techniques such as "stop and frisk").

[53] *See e.g., id.* at 604 ("Police used deceptive and coercive interrogation practices to interview juveniles Larry and Calvin Ollins, Omar Saunders, and Marcellius Bradford, and facilitating in them blaming each other.").

acknowledging their negligence or lack of due diligence.

The same phenomenon is observed in the United Kingdom. In the United Kingdom, young Black people are featured easily in the gang database, even if these people did not commit the crimes.[54] This could lead to discriminatory practices similar to those in the United States. In France, while no percentage has been released, non-white people were particularly targeted after the November 13, 2015 attacks in Paris, and policing measures singled them out according to Jacques Toubon, former Défendeur des droits.[55]

When FRT is used by law enforcement for preventative policing, Black people are disproportionately affected.[56] In 2016, Detroit planned a project called Green Light, where facial recognition technology was installed in eight separate gas stations all over the city—but the cameras are mainly situated in predominantly Black population areas, resulting in over-policing and criminalization of Black people.[57] Not only might these practices further severely affect Black people since potential employers and landlords might have access to their criminal records and might refuse to provide them jobs or housing in the future, but these discriminatory practices also affect human rights at their core.[58]

[54] *Trapped in the Gangs Matrix*, AMNESTY INT'L U.K. (Nov. 23, 2018, 11:21 AM), https://www.amnesty.org.uk/trapped-gangs-matrix.

[55] *15 Things to Know about Racism and Police Brutality in France*, TRTWORLD (2017), https://www.trtworld.com/europe/do-french-police-have-a-race-problem-302154.

[56] *See* Kristian Lum & William Isaac, *To Predict and Serve?*, SIGNIFICANCE MAG., Oct. 2016, at 15 (raising the concern that police-recorded data is racially biased and could result in discriminatory policing).

[57] Rebecca Smith, *Project Green Light: Surveillance and the Spaces of the City*, UNIV. MICH. CARCERAL STATE PROJECT (2021), https://storymaps.arcgis.com/stories/14dd97b35cbb4a4298786c75855f8080.

[58] *See* Rachel Kleinman & Sandhya Kajeepeta, *Barred from Work: The Discriminatory Impacts of Criminal Background Checks in Employment*, THURGOOD MARSHALL INST. (Apr. 2023), https://tminstituteldf.org/criminal-background-checks-employment/#:~:text=Given%20the%20racial%20discrimination%20embedded,imported%20into%20the%20employment%20sphere ("Given the racial discrimination embedded in the criminal legal system, the use of criminal background checks disproportionately excludes Black people from employment. Through criminal background check policies, racial discrimination in the criminal legal system is compounded and imported into the employment sphere."); Press Release, New Report Examines How Abuse and Bias in Tenant Screening Harms

Even if the FRT algorithms are "de-biased," human nature will never be "de-biased." The usage of FRT therefore reinforces, perpetuates, and legitimizes the action of law enforcement against people of color. These practices lead to the violation of the human rights of Black people, which Part III will focus on.

III. HUMAN RIGHTS' IMPACTS

Facial technology disproportionately violates the human rights and freedom of people of color at the regional, national, and international levels. This section will focus on and analyze the most impacted of these rights, such as the right to privacy, the right to assembly, and the right to free speech.

A. RIGHT TO PRIVACY

Privacy protects individuals against undue governmental interference in their personal lives.[59] This includes the protection against the surveillance and search of persons and areas where people have a reasonable expectation of privacy unless there is a sufficient justification for government intrusion.[60] In short, this is the "right to be left alone," unless an imperative interest might justify the intrusion, such as public safety. Privacy is a right largely recognized by international and regional human rights institutions. The United Nations discusses this right in Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[61] Article 8 of the European

Renters, NAT'L CONSUMER L. CTR. (Sept. 26, 2023), https://www.nclc.org/new-report-examines-how-abuse-and-bias-in-tenant-screening-harm-renters ("Landlords in the United States almost always engage in some form of automated screening of rental applicants . . . screening process is riddled with errors and bias that disproportionately harms Black and Latino/Hispanic renters."); Ozasvi Amol, *Wrongful Convictions – A Malady for the Criminal Justice System*, AMICUSX (Dec. 9, 2021), https://www.amicusx.com/post/wrongful-conviction-a-malady-for-the-criminal-justice-system (arguing that wrongful conviction is violation of human rights).

[59] *See* Katz v. United States, 389 U.S. 347, 347, 360–61 (1967) (Harlan, J., concurring) (joining in the majority opinion that where a person has both a subjective and objective expectation of privacy the government cannot interfere without a warrant).

[60] *Id.* at 359.

[61] *See* International Covenant on Civil and Political Rights, art. 17, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR] (stating that no one shall be subjected

Convention on Human Rights (ECHR) and Article 7 of the EU Charter of Human Rights also mention the right to privacy.[62] Further, the right to privacy has been implied in the Fourth Amendment of the U.S. Constitution, according to U.S. Supreme Court case law.[63] All of these laws aim to ensure that individuals have a reasonable right to privacy from the government, including from law enforcement. However, the installation of surveillance cameras in streets and public spaces threatens the right to privacy, and the anonymity that privacy aims to protect.

By classifying crowds, individuals are identified, recognized, and exposed to the threat that their data will be collected, stored, and used by law enforcement. The collection of vulnerable data violates the right to privacy as law enforcement can investigate and divulge personal information about people. With technology, the individual's privacy is at risk. Black people will be the first to suffer from these technological threats. As discussed earlier, Black people are more at risk by preventive policing and the installation of FRT.[64] In this context, people of color are more at risk of being identified while they are only walking in the streets, and have their data and anonymity violated, whereas white people traversing in another neighborhood might be left alone.

Further, the high rate of misidentification for Black people "will likely result in more governmental interventions and interactions" for

to arbitrary or unlawful interference in their privacy).

[62] *See* Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), art. 8, Nov. 4, 1950, 213 U.N.T.S. 221, E.T.S. No. 5 [hereinafter ECHR] (reiterating rights to individual privacy in one's private life, family life, and correspondences); Charter of Fundamental Rights of the European Union, art. 7, 2012 O.J. (C326) 397 [hereinafter "EU Charter"] (declaring that State Parties must have respect for private and family life).

[63] *See* Rory Little, *Protecting Privacy under the Fourth Amendment*, 91 YALE L.J. 313, 313–14 (1981) (highlighting how since the mid-nineteenth century, cases like Katz have protected the right to privacy under the Fourth Amendment of the U.S. Constitution).

[64] *See* Thomas et al., *supra* note 46 ("An analysis of arrest data voluntarily reported to the FBI by thousands of city and county police departments around the country reveals that, in 800 jurisdictions, black people were arrested at a rate five times higher than white people in 2018, after accounting for the demographics of the cities and counties those police departments serve.").

Black people.[65] When a false positive identification of a Black person occurs, it leads to a collection of sensitive information such as fingerprints and mugshots which could result in the breach of the right to privacy without justification. These results will result in more violations of human rights by law enforcement for Black people.

Unfortunately, this intrusion of people's privacy might lead to dramatic consequences. Indeed, more than the violation of privacy, which is already a significant violation of human rights, people of color might lose their right to housing if a record of their criminal past is required by the landlord or to qualify for state aid.[66] Additionally, some people of color might lose their right to exercise a profession. For instance, to be admitted to practice law, a candidate must show good fitness and as part of that fitness test, a past conviction, even wrongful, might lead to the non-admission of the candidate to the bar exam.[67] Unfortunately, the right to privacy is not the only right affected by facial recognition. The right to assembly is also under threat.

B. THE RIGHT OF ASSEMBLY AND FREE SPEECH

The right to assembly guarantees the right for people to assemble peacefully for any purpose that is not prohibited by law.[68] Right to assembly can be a platform to advocate for changes in their society. In Europe, freedom of assembly is protected under various laws, such as Article 21 of the International Covenant on Civil and Political Rights, Article 11 of the European Convention on Human Rights, and Article

[65] Lindsey Jacques, *Facial Recognition Technology and Privacy – How to Ensure the Right to Privacy is Protected*, 23 SAN DIEGO INT'L L.J. 111, 120, 126–27 (2021).

[66] *See* Jaboa Lake, *Preventing and Removing Barriers to Housing Security for People with Criminal Convictions*, CTR. FOR AM. PROGRESS (Apr. 14, 2021), https://www.americanprogress.org/article/preventing-removing-barriers-housing-security-people-criminal-convictions ("As of 2021, the National Inventory of Collateral Consequences of Conviction identifies more than 1,300 criminal record-related barriers to housing and residency across state, county, and city jurisdictions, and 26 barriers at the federal level.").

[67] *Understanding the Bar Exam Character and Fitness Process*, BARBRI (Jan. 17, 2022), https://www.barbri.com/blog/usbar/understanding-the-bar-exam-character-and-fitness-process.

[68] ECHR, *supra* note 62, art. 11 § 2.

12 of the European Union's Charter of Fundamental Rights.[69] In the U.S., under the First Amendment to the Constitution, Americans have a right to freely express themselves and assemble peacefully.[70] The right to assembly is a fundamental component of a democratic state.[71] Without its guarantee, governments may act without consulting and listening to their people and might lead the state to tyranny.[72] Thus, the right of assembly must be protected in democratic countries. Nevertheless, facial recognition may violate this fundamental right.

Law enforcement uses facial recognition to monitor protests and protect public safety.[73] Therefore, the technology could potentially lead to the identification of people protesting in the streets. Facial recognition might be used to control people's behaviors. Consequently, individuals might decide not to participate in rallies or to not express themselves the way they want. Thus, it has a chilling effect on the rights of freedom of speech and the right to assemble. Courts have found that facial recognition might affect the right to assemble. In the case, *La Quadrature du Net*,[74] the European Court of Justice declared that the general retention of data was a violation of Article 11 of the E.U., Charter on Human Rights, i.e., the right to freedom of expression. Similarly, a German court declared the publication of pictures illegal during a protest because it can have a

[69] Marya Akhtar, *Police Use of Facial Recognition Technology and the Right to Privacy and Data Protection in Europe,* 9 NORDIC J. L. & SOC. RSCH. 325, 339 (2019).

[70] U.S. CONST. amend. I.

[71] *See* ICCPR, *supra* note 61, art. 21 ("The right of peaceful assembly shall be recognized. No restrictions may be placed on the exercise of this right other than those imposed in conformity with the law and which are necessary in a democratic society. . . .").

[72] *See* Human Rights Comm., General Comment No. 37 on the right of peaceful assembly (article 21), U.N. Doc. CCPR/C/GC/37 at ¶¶ 1–2 (2020) [hereinafter "ICCPR General Comment 37"] (asserting that the right to peaceful assembly is essential in respecting and ensuring that the government is based on rule of law and pluralism, not repression).

[73] *See* Lee Rainie, et al., *Public More Likely to See Facial Recognition Use by Police as Good, Rather than Bad for Society*, PEW RSCH. CTR. (March 17, 2022), https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society.

[74] Case C-511/18 and C-512/18, La Quadrature du Net and Others v. Premier Ministre, ECLI:EU:C:2020:791, ¶ 125 (Jan. 15, 2020).

negative impact on the right to assembly.[75]

People of color are disproportionately affected by these practices. In 2020, during the Black Lives Matter (BLM) protests in Baltimore, Maryland, Baltimore Police were reported to have used facial recognition by linking the images to social media profiles.[76] Additionally, the New York Police Department (NYPD) used facial recognition to track down BLM protesters.[77] While data in Europe is lacking, in Russia, the Russian authorities used facial recognition to identify people protesting in support of President Vladimir Putin's opponent, Alexei Navalny.[78] Researchers have shown that Russian facial recognition companies have built tools to detect a person's face.[79] One can assume that the use of facial technologies during a protest against Putin and Russia's politics towards minorities and immigrants might deter people of color from participating in a protest. In Europe and the United States, facial recognition threatens the right of assembly of people of color since they might be more surveilled and therefore less inclined to participate in a protest.

The right to peaceful assembly ensures the citizen's participation in the political life of a country. It ensures democracy and the right of

[75] Case 14 K 3543/18, Verwaltungsgericht Gelsenkirchen [Administrative Court of Gelsenkirchen] ECLI:DE:VGG E:2018:1023, ¶¶ 56, 58, 60–61, 65 (Oct. 23, 2018) (Ger.) [hereinafter "Gelsenkirchen"].

[76] *See* Shira Ovide, *A Case for Banning Facial Recognition*, N.Y. TIMES (Aug. 1, 2021), https://www.nytimes.com/2020/06/09/technology/facial-recognition-software.html (explaining why facial recognition services is dangerous when used for law enforcement purposes because it is detrimental to specific groups of people).

[77] *See USA: NYPD Ordered to Hand over Documents Detailing Surveillance of Black Lives Matter Protests following Lawsuit*, AMNESTY INT'L (Aug. 1, 2022), https://www.amnesty.org/en/latest/news/2022/08/usa-nypd-black-lives-matter-protests-surveilliance/#:~:text=The%20New%20York%20Police%20Department, the%20Surveillance%20Technology%20Oversight%20Project (discussing a New York Supreme Court case that holds the New York Police Department had to disclose how it obtained and used the facial recognition data it procured during the Black Lives Matter movements).

[78] *See* Umberto Bacchi, *Fears Raised Over Facial Recognition Use at Moscow Protests*, REUTERS (Feb. 4, 2021, 7:48 AM), https://www.reuters.com/article/russia-protests-tech-idUSL8N2KA54T (noting that the facial recognition technology is being used to "stifle peaceful dissent").

[79] *See* Umberto Bacchi, '*Racist' Facial Recognition Sparks Ethical Concerns in Russia*, REUTERS (July 5, 2021, 1:51 PM), https://www.reuters.com/article/uk-russia-tech-race-idUSKCN2EB0BC (describing facial recognition technology as "purpose-made for discrimination").

every citizen to equally be heard. However, facial recognition has an obvious "chilling effect" on the right of assembly since people of color might decide not to engage in the politics of their country and feel persecuted by authorities.[80] Thus, there may be a discriminatory and negative effect on the trust that people of color have in law enforcement and governmental institutions.[81]

On this matter, the U.N. Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association has stated that the use of surveillance techniques for arbitrary surveillance of individuals exercising their freedom of assembly should be prohibited.[82] The Special Rapporteur notes that this chilling effect may be aggravated if the demonstration concerns views that differ from the majority view.

Thus, the use of facial recognition will have a disproportionate impact on people of color. FRT inaccurately recognizes people which replicates and emphasizes existing discrimination and promotes violations of human rights. The next section will focus on the current legal frameworks of the United States and Europe covering FRT and emphasizes the insufficiencies of the current regulations.

IV. THE INSUFFICIENCIES OF THE CURRENT REGULATIONS REGARDING FACIAL RECOGNITION

Police use of facial technology can certainly help to identify suspects. However, as examined in Part III, human rights and liberties are harmfully impacted by its use. Aware of this issue, several countries have proposed regulations. Yet, only a few countries, such

[80] *See* Jake Laperruque, *Facing the Future of Surveillance — Task Force on Facial Recognition Surveillance*, POGO, (Mar. 4, 2019), https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance (noting that this type of surveillance even has an impact on a person's daily activities).

[81] *See* European Union Agency for Fundamental Rights (FRA), *supra* note 28 at 10 (detailing that this low trust and overall group cohesion is because specific ethnic groups are disproportionately impacted by the facial recognition technology).

[82] *See* U.N. High Commissioner for Human Rights, *Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peace Protests*, 8, U.N. Doc. A/HRC/44/24 (June 24, 2020) (noting that facial recognition technology is exchanged worldwide, making it available to a wide range of uses).

as Belgium[83] and Luxembourg,[84] have instituted a ban on facial responses. Many countries still allow facial recognition without sufficient safeguards.[85] This section will emphasize that no country has implemented impactful regulations on facial recognition to eliminate these human rights violations. Human rights law and data privacy regulate facial recognition, but without tackling its racial bias.

Since 2018, the European Union has implemented the most stringent regulations on data privacy with the General Data Protection Regulation (GDPR), which also covers biometric data.[86] Article 4 states that personal data resulting from special treatment, relating to physical, psychological, or behavioral characteristics of a physical person, permits and confirms their unique personality.[87] Indeed, the definition set forth in Article 4 encompasses biometric data since it permits the collection of the physical characteristics of individuals. Due to their nature, and the information they contain, GDPR imposes more safeguards and restrictions for the processing of biometric data.[88] Article 9 of the GDPR prohibits the use of sensitive data.[89] The use of sensitive data is prohibited because it reveals the race or religious opinions of a person. In this case, the individuals must consent to the treatment of the data. The consent must be free, unequivocal, and

[83] *See* Charles Rollet, *Belgium Bans Private Facial Surveillance*, IPVM (July 6, 2018, 08:29 AM), https://ipvm.com/reports/belgium-biometrics (stating that the use of biometric-based video analytics, such as face recognition, in surveillance cameras for non-police, private purposes has been prohibited in Belgium).

[84] *See* Jess Bauldry, *Lux Police Not Using Facial Recognition*, DELANO (Aug. 22, 2019), https://delano.lu/article/delano_lux-police-not-using-facial-recognition (detailing the ban on facial recognition technology even extends to some police usage in Luxembourg).

[85] *See also* Kamalika Some, *Which Countries Allow and Which Ban AI Facial Recognition*, ANALYTICS INSIGHT (Aug. 14, 2020), https://www.analyticsinsight.net/countries-allow-ban-ai-facial-recognition (explaining that China dominates the market for facial recognition, and is even exporting it all around the world).

[86] *See What is the GDPR, The EU's New Data Protection Law?*, GDPR, https://gdpr.eu/what-is-gdpr (explaining how the GDPR is the strictest privacy regulation in the world, and despite its creation and approval by the European Union, it places requirements on companies worldwide as long as they gather information about individuals within the EU).

[87] Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) art. 4 [hereinafter GDPR].

[88] *Id.* art. 9.

[89] *Id.*

explicit that the individual has accepted the treatment of their data.[90] In the E.U., people of all races must therefore consent to the collection of their data, otherwise, it might constitute a violation of the GDPR. For instance, in 2020, an administrative court of Marseille declared an experimental system of facial recognition in a high school in violation of GDPR.[91] The court stated that the system did not offer sufficient tools and safeguards for explicit consent by the students.[92] Indeed, the explicit consent of people might lead to a smaller use of biometric data and protect people of all races' privacy, therefore limiting the racial bias of facial recognition. However, the invasive nature of facial recognition does not currently permit the collection of explicit consent.[93] Biometric data might be collected from social media without the consent of the individual, and then be used by law enforcement. Today, as more social media sites and large corporations have implemented facial recognition, people might agree implicitly or not at all. Here, the GDPR does not implement sufficient safeguards and tools for the generalization of facial recognition because people might not consent to have their data collected, and people of color might still suffer from the racial bias of facial technology and racial bias by the police. Although the GDPR was a significant first step in safeguarding FRT's use, facial recognition needs a stronger legal framework.

Article 14 of the ECHR may also help protect people of color against the biases of facial recognition.[94] The article sets forth that, "the enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination."[95] The article prohibits all measures that would be discriminatory against human rights protected by the Convention, such as the right to privacy and the right to

[90] *Id.*

[91] Tribunal Administratif [TA] [regional administrative court] Marseille, 9e civ, Feb. 27, 2020, No. 1901249 (Fr.).

[92] *Id.*

[93] *See* Consultative Comm. of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), Guidelines on Facial Recognition, 9, 11 (June 2021). (explaining that the power imbalance between those collecting the data and those whom the data is being collected from would render consent mute).

[94] ECHR, *supra* note 62, art. 14.

[95] *Id.*

assembly. Member States must comply with the measures implemented by the ECHR, or they will be condemned. For example, in *R (on the application of Edward Bridges) v. The Chief Constable of South Wales Police*,[96] the Court of Appeals found that facial recognition software used by the South Wales Police violated the principle of anti-discrimination since the technology generated a higher proportion of false positive matches for minority groups. Therefore, Article 14 of the ECHR may be a tool to condemn and call on States to revise their regulations. However, States do not effectively implement the provisions of the ECHR.[97] States retain a margin of appreciation to modify their legal system to enforce the ECHR rulings. Therefore, since States might decide to bypass judicial decisions, the ECHR might only have a slight impact on tackling, and may even welcome, racial biases within FRT.

Further, States have tried to implement tools to tackle facial recognition abuses. In 2019, the European Council adopted Convention 108+ on the Protection of Individuals with Regard to the Processing of Personal Data.[98] In Article 6, the use of facial recognition to determine the race or religion of an individual is prohibited unless significant safeguards are ensured.[99] Article 6 of Convention 108+ states that processing biometric data identifying individuals requires appropriate safeguards.[100] Parties must prevent any risk that the processing of sensitive data can adversely affect the interests and rights of the individual, especially discriminatory risk.[101] To ensure the lawfulness of the processing, the party must take reasonable measures in case of an accidental disclosure and must ensure that the response must know the potential effect of the data

[96] R v. the Chief Constable of South Wales Police, [2020] EWCA Civ 105 [94, 95, 200–01] (U.K.).

[97] CEDRIC BOUTY, *Chose jugée –Décisions bénéficiant ou ne bénéficiant pas de l'autorité de la chose*, *in* REPERTOIRE DE PROCEDURE CIVILE, ¶ 354 (Dalloz 2018).

[98] Council of Europe, Amending Protocol to Modernised Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 5, May 18, 2018, C.E.T.S. No. 223 [hereinafter Convention 108+].

[99] *Id.* art. 6.

[100] *Id.*

[101] *See* Akhtar, *supra* note 69 at 339 (examining the precise guidelines under the Convention that safeguard individuals whose biometric data has been gathered).

proceedings on fundamental rights.[102] These tools aim to prevent any violation of human rights. Even if this detailed convention might prevent and limit the impacts on human rights when FRT is involved, States have not enacted stronger legislation regulating FRT. On the contrary, countries like France want to amplify their use of experimental FRT.[103] Despite the advancement of protection of personal data, the Convention does not contain any regulation or obligation on accuracy and racial bias in FRT, which leaves the issue of racial bias in FRT unaddressed and unresolved. Despite the desire from States to pass regulations on the matter, most of them are still in negotiations. Currently, European countries are not the only region lacking stringent and specific regulations on the matter. The U.S. is currently in a similar position as most European countries.[104]

At the federal level, the U.S. Congress has not yet passed legislation on FRT.[105] While the U.S. Constitution and other statutes could fill this legal void, they have not yet yielded a satisfactory response. FRT's impact on human rights might raise challenges regarding the Fourth and Fourteenth Amendments. The Fourth Amendment of the U.S. Constitution protects against unreasonable searches and seizures, which limits police interference with people's privacy.[106]

The U.S. Supreme Court recognized that when there is a reasonable expectation of privacy for an individual, the search requires a warrant

[102] *See* i*d.* (noting that Article 6 of the Convention states that the act of processing biometric data that identifies an individual is only permitted when the relevant legal protections are in place).

[103] *See also* Masha Borak, *French Senate Votes in Favor of Public Facial Recognition Pilot*, BIOMETRIC UPDATE (June 24, 2023, 8:27 PM) https://www.biometricupdate.com/202306/french-senate-votes-in-favor-of-public-facial-recognition-pilot (noting that the French Senate recently passed a law allowing the use of facial recognition technology in public spaces).

[104] *See also* Skye Witley & Andrea Vittorio, *Facial Recognition Software is Everywhere, With Few Legal Limits*, BLOOMBERG L. (Apr. 27, 2023, 4:55 AM) https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/X9BS35M8000000?bna_news_filter=privacy-and-data-security#jcite (discussing a proposed New York bill that would ban businesses from tracking customers by using facial recognition technology, which would be the second law in the United States banning this type of technology).

[105] *See also id.* (noting that there is no federal law limiting the power of facial recognition technology).

[106] U.S. CONST. amend. IV.

unless an exception exists.[107] The Supreme Court has crafted the Fourth Amendment to limit seizures and arrests by requiring reasonable suspicion to justify an arrest.[108] In that sense, officers must be able to point to specific and articulable facts taken together with rational interference from those facts that reasonably warrant that intrusion.[109] The Supreme Court has never quantified how police might be mistaken or how low the threshold for error should be set.[110] The courts have never specified the level required to have a reasonable suspicion.[111] Therefore, for FRT, this uncertainty means that the error rate for a match could be significant, yet constitutional.[112] Currently, like in the case of Mr. Williams, a victim may not obtain relief because since there was recognition by the technology, that could therefore be understood as reasonable suspicion by police officers.

Additionally, the Fourth Amendment tolerates errors from law enforcement and restricts civil and criminal remedies.[113] Police must have a sound and justified suspicion. Yet, police officers can also make mistakes in identification, especially if the decision is "an objectively 'reasonably good-faith belief' that their conduct is

[107] Heien v. North Carolina, 574 U.S. 54, 61–62 (2014) ("To be reasonable is not to be perfect, and so the Fourth Amendment allows for some mistakes on the part of government officials, giving them "fair leeway for enforcing the law in the community's protection.'"); Missouri v. McNeely, 569 U.S. 141, 148 (2013).

[108] *See* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1174 (2021) (describing the standard of "reasonable suspicion" as a low bar for the police to stop and seize someone).

[109] *See* Ric Simmons, *Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in Our Criminal Justice System*, 2016 MICH. ST. L. REV. 947, 1011 (2016) (noting that both reasonable suspicion and probable cause require an officer to point to specific facts to show the individual was likely involved in criminal activity).

[110] *See id.* at 964 (noting that the Supreme Court and some lower courts have hinted at the sentiment that probable cause does not equate to "more probable than not," meaning the standard is likely less than fifty percent).

[111] *See id.* (explaining that "[a]lthough courts have been unwilling to explicit quantify the percentage for 'reasonable suspicion,'" it is likely more than twelve percent, but less than fifty percent).

[112] *See* Ferguson, *supra* note 108 at 1176 (stating that facial recognition technology can produce both false positives and false negatives, meaning individuals could be stopped based on errors).

[113] *See id.* at 1179 (noting that the reasonable suspicion threshold and the probable cause threshold allow large margins for errors).

lawful"[114] or when the mistake was not intentional, reckless, grossly negligent, or systemic.[115] Even if a victim could argue that the police were negligent by not conducting further research and verifying where the suspect was at the time of the incident, police officers may nonetheless not be liable since the officers were merely negligent rather than acting in bad faith. Under the precedents set by the Supreme Court of the United States, mere negligence is not sufficient to prove criminality, and neither will it award civil damages for victims.[116] Therefore, the Fourth Amendment does not offer sufficient protection to people of color to tackle the discrimination suffered through FRT use. Moreover, the Fourth Amendment may not be the proper avenue to address racial bias. The Supreme Court has refused to address racial bias under the Fourth Amendment: the Court has held that the constitutional basis for objecting to intentionally discriminatory application of the law is the Equal Protection Clause, not the Fourth Amendment.[117] Therefore, it is unlikely that a person of color will get redress under the Fourth Amendment. Therefore, in line with the *Whren*[118] decision, the next part will examine the possibilities of tackling racial bias under the Fourteenth Amendment.

Another provision that may protect racial discrimination is the Equal Protection Clause of the Fourteenth Amendment.[119] The Equal Protection Clause and Due Process might be violated by the racial discrimination involved in facial recognition technology. A claim will be sustained if the plaintiff proves the FRT has a discriminatory effect and purpose.[120]

The first element, discriminatory effect, is usually easier to prove. As discussed above, several studies have established bias in facial recognition where people of color are more at risk of being

[114] Davis v. United States, 564 U.S. 229, 238 (2011).
[115] Utah v. Streiff, 136 S. Ct. 2056, 2058 (2016).
[116] *Davis*, 564 U.S. 238 (2011).
[117] Whren v. United States, 517 U.S. 806, 813 (1996) ("We of course agree with petitioners that the Constitution prohibits selective enforcement of the law based on considerations such as race. But the constitutional basis for objecting to intentionally discriminatory application of laws is the Equal Protection Clause, not the Fourth Amendment.").
[118] *Id.*
[119] U.S. CONST. amend. XIV, § 1.
[120] Washington v. Davis, 426 U.S. 229, 237 (1976).

misidentified than white people. Therefore, since a part of the population is more at risk of suffering from discrimination, the first element is met.[121]

The second element, discriminatory purpose, is more difficult to prove.[122] One feature must be that facial recognition is intentionally targeted directly at people of color. Here, general statistics may not be enough to prove discriminatory purposes. The intent of law enforcement to target people of color is necessary for this element. It might be difficult to prove the implicit bias of a police officer or a racist act. First, the police officer may not expressly say that he stops a person because of his race. Thus, it might be difficult to argue that the arrest had a discriminatory purpose. In addition, as previously mentioned, people may not be aware of their own bias against people from another ethnic minority under the own-race effect. Because of this, it might be very difficult to prove that an officer had a discriminatory intent.[123] Further, an officer might act relying solely on facial recognition, and not for an intentional discriminatory purpose. Therefore, it may be difficult to rely on that element to prove a discriminatory purpose. This means that people of color may be unlikely to obtain redress under the Fourteenth Amendment since they cannot prove the discriminatory intent of facial recognition.

Unfortunately, current statutes and laws might not help to tackle racial bias because they are ill-designed to grasp the nature of facial recognition. In 2002, the U.S. Government passed the E-Government Act to protect personal information contained in government records and systems.[124] Under Section 208 of the E-Government Act, Privacy Impact Assessments (PIA) are required for all federal government agencies that develop or procure new information technology involving the collection, and maintenance of information in

[121] *See* Eldar Haber, *Racial Recognition*, 43 CARDOZO L. REV. 71, 110 (2021) ("[T]he statistical or otherwise aggregated data for accuracy rates of the technology and, more specifically, against some minorities could aid in proving discriminatory effect").

[122] *See id.* at 111 (identifying why discriminatory purpose is more difficult to prove).

[123] *See id.* (discussing the subconscious shortcomings that result from cognitive bias).

[124] *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899.

identifiable form.[125] The PIA system is used to demonstrate that system owners have incorporated privacy protections throughout the entire life cycle of a system. Therefore, by ensuring sufficient protection, data from people of color might not be leaked to unauthorized people or companies. However, PIA validations are not conducted as regularly as they should be.[126] Therefore, risks remain present in the use of FRT. The impact of such regulations, while welcomed, is only minimal.

Civil rights law might not help on the matter. The Title VI provision of the Civil Rights Act of 1964 prohibits recipients of federal financial assistance from discriminating based on race, color, or national origin in their programs or activities.[127] The U.S. Department of Homeland Security funds grants for state and local governments to purchase and use facial recognition technology. Therefore, the racial biases of facial recognition technology might be denounced under the Civil Rights Act since law enforcement received grants from the federal government.[128] However, anti-discrimination laws are rarely used against racist police practices, and, unfortunately, the disparate impact doctrine might not be helpful.[129] The disparate impact doctrine is used when a policy or law disproportionately impacts a community because of its race or religion. For facial recognition, studies have demonstrated that certain people might be particularly targeted because of their race or color. However, the theory is not considered for criminal enforcement.[130]

Therefore, despite several concerns with data privacy and human rights, States do not regulate the use of facial recognition sufficiently.

[125] *E-Government Act of 2002*, U.S. DEP'T OF JUST. OFF. OF PRIV. AND CIV. LIBERTIES (Feb. 13, 2019), https://www.justice.gov/opcl/e-government-act-2002.

[126] Haber, *supra* note 121, at 115.

[127] 42 U.S.C. § 2000d.

[128] *See* Margaret Ulle, *How Are States Responding to Facial Recognition Surveillance*, POGO (Aug. 15, 2019), https://www.pogo.org/analysis/how-are-states-responding-to-facial-recognition-surveillance (describing federal grants to law enforcement agencies for facial recognition technology).

[129] *See* Haber, *supra* note 121, at 114 ("Unfortunately, antidiscrimination laws are rarely used to create any systematic change within already discriminatory and racist police practices.").

[130] *See id.* ("While some argue that disparate impact laws must apply to criminal enforcement, the disparate impact doctrine is not yet considered part of criminal enforcement.").

Further, there is persistent inaccuracy in facial recognition technology and its use by law enforcement agencies. In the final section, we will examine which solutions might be considered by the States to address the racial bias against facial recognition.

V. PROSPECTIVE MEASURES AND LEGISLATIONS ON FACIAL RECOGNITION'S USE BY LAW ENFORCEMENT

Because several studies have established facial recognition bias, as well as China's instauration of a very intrusive facial recognition system, many states have discussed regulations on facial recognition technology.[131] With the development and abuses of technology, governments are more pressured to act, not only by society but also by private companies, such as Amazon.[132] But the question now is what will such regulations look like?

Current proposals range from a total ban to a moratorium of certain use by law enforcement and commercial entities.[133] To stop the negative impact of facial recognition would mean to ban the technology. However, the possibility of such an option might be difficult to implement. Indeed, facial recognition has expanded tremendously through the years, especially in airports, on our smartphones, and on city streets. Banning facial recognition technology would mean eliminating identity recognition controls at airports and criminalizing a technology in which states have heavily

[131] *See* Tambiama Madiega & Hendrik Mildebrath, European Parliamentary Research Service (EPRS), *Regulating Facial Recognition in the EU*, 33 (2021) (highlighting concerns to regulate the use of facial recognition technology).

[132] *See* Joseph Pisani, *Amazon Halts Police Use of Its Facial Recognition Technology For a Year*, OPB (June 10, 2020), https://www.opb.org/news/article/facial-recognition-police-amazon("Amazon . . . banned police use of its face-recognition technology for a year, making it the latest tech giant to step back from law-enforcement use of systems that have been criticized for incorrectly identifying people with darker skin.").

[133] *See* Taylor Kay Lively, *Facial Recognition in the United States: Privacy Concerns and Legal Developments*, ASIS INT'L (Dec. 1, 2021), https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2021/december/facial-recognition-in-the-us-privacy-concerns-and-legal-developments (discussing current proposals for federal level facial recognition regulation, including the Facial Recognition and Biometric Technology Moratorium Act of 2021).

invested.[134] Even if a ban would be the most effective way to protect human rights, facial recognition technology has widened too quickly to be stopped now. In addition, with a total prohibition of facial recognition, black market demand might rise.[135] Authorities would not have the power to regulate it which might lead to more harmful use by private individuals and organizations that might cause greater harm to people of color.[136] Additionally, white supremacist groups might use it to target people of color or illegal immigrants in order to victimize them.[137] Therefore, a ban might not be the best solution to protect minorities. Further, economically, a ban on facial recognition would not be the most adequate answer.[138] Yet, a regulatory framework is needed. There are other legal solutions that can help mitigate the negative impacts of the technology.

A comprehensive moratorium on FRT is a solution being considered by the E.U. The European Parliament invited the Commission to consider a moratorium on FRT in public on its deployment. In its paper, the European Commission proposes a prohibition on high-risk real-time remote identification systems for law enforcement purposes.[139] However, exceptions might be provided for the use of real-time remote biometric identification systems, such as an imminent terrorist attack. A moratorium will stop all innovations

[134] *See* Jacques, *supra* note 65, at 140 (outlining the pervasive reliance on facial recognition technology that has developed across various agencies and institutions throughout the U.S.).

[135] *See id.* at 148 (noting the risk of heightened black-market demand for FRT following a ban, in addition to an already existing market in Russia in the absence of a ban).

[136] *See id.* at 148–49 (arguing why a ban is not the best solution to protect marginalized sections of the community in the U.S.).

[137] *See id.* at 149 (demonstrating the essential role of Facial Recognition Technology in combatting crime, white supremacism, extremism, and the targeting of racial minorities).

[138] *See* Ryan Browne, *Tech Giants Want Rules on Facial Recognition, but Critics Warn that Won't be Enough*, CNBC (Aug. 30, 2019), https://www.cnbc.com/2019/08/30/facial-recognition-tech-firms-want-regulation-but-critics-want-a-ban.html (contending that a ban is not the answer, and instead that regulation plus securing data when it is collected and handled is a more complete answer).

[139] Madiega & Mildebrath, *supra* note 131, at 25 ("[T]he immediacy of the remote identification and the limited redress mechanisms available to individuals increases the risks for the rights and freedoms of the persons that are concerned by law enforcement activities.").

and development of facial recognition technology by companies. However, a moratorium does not mean the correction of the existing bias contained in the technology. To be effective and tackle racial discrimination, in addition to the moratorium, legislators should impose technologies to correct the bias.

The first step that might lead to a fairer system is to have a human review FRT results before they are utilized. For example, Mr. Williams was arrested and convicted even though he was not at the place of the incident. If someone had verified the results of the facial recognition system, the mistake might have been overridden and avoided. It is worth noting that it may be effective to have a person from the same race as the individual analyzing the results.

Second, as stated in Part II, databases are disproportionately composed of pictures of white men. Ensuring more diverse databases that represent all minorities will limit the misidentification of people of color. Additionally, governments should regulate the codes to avoid any bias in it. Technology is biased because codes are designed by engineers and humans are inherently biased. Correcting the bias could help correct the inaccuracy of the technology. On this matter, States should issue guidelines and evaluate the software to test its accuracy and the biases that might occur.[140]

In this sense, the European Union is considering certain procedural safeguards. In the proposed regulation, the E.U. is considering regulating the use by following a risk-based approach.[141] An ex-ante and ex-post evaluation of technology should be done by the providers. In an ex-ante evaluation,[142] providers would include the assessment of the quality management system and the assessment of the technical

[140] *See* Sam duPont, *Facial Recognition Is Here but We Have No Laws*, NEXTGOV (July 8, 2020), https://www.nextgov.com/ideas/2020/07/facial-recognition-here-we-have-no-laws/166711 ("[T]o address bias risks, Congress should establish testing requirements, standard-setting, and certification mechanisms to prevent deployment of biased facial recognition systems.").

[141] Madiega & Mildebrath, *supra* note 131, at 24 ("The Commission proposes to enshrine a technology-neutral definition of AI systems in EU law and to lay down a classification for AI systems with different requirements and obligations tailored on a 'risk-based approach.'").

[142] *See id.* at 27 ("In principle, AI systems used for biometric identification would need to undergo conformity assessment by an independent body . . . unless harmonised standards or common specifications exist.").

documents of the designated AI system. The proposed legislation would require a documented risk-mitigation process to prevent harm which could tackle racial bias in the technology. By introducing a requirement for the quality of processes, providers will have to ensure more neutral codes and pay attention to racial bias. The implementation of a third independent party is another way to ensure that the assessment will be conducted properly without any bias. To ensure compliance with regulations, States might institute a third-party authority, like a Data Protection Officer (DPO),[143] who could provide oversight as to the compliance of FTR with regulations.

In the U.S., a total ban on facial recognition has been introduced by Senators Ed Markey and Jeff Merkley[144] and House of Representatives Pramila Jayapal and Ayanna Pressley.[145] Several cities, such as Oakland, San Francisco, and Boston, have banned facial recognition.[146] However, as previously mentioned, a nationwide ban might be difficult, especially in certain areas like airports.

As discussed above, in the U.S., technology has developed very quickly and its use by law enforcement is widespread, leading to more harm to people of color. Like in the E.U., the U.S. should try to correct the bias and inaccuracy of facial recognition. A potentially effective way for the United States to regulate FRT is a moratorium to limit the bias that people of color might experience. To address this, the United States must pass strict and precise regulations to correct inaccuracy and discriminatory effects. A regulation on data privacy might not be enough, because as seen with the GDPR, a regulation acknowledging

[143] *See* GDPR, *supra* note 87, art. 43 (outlining the tasks of a data protection officer).

[144] *See Senators Markey and Merkley Lead Colleagues on Legislation to Ban Government Use of Facial Recognition, Other Biometric Technology*, ED MARKEY, U.S. SEN. FOR MASS. (June 15, 2021), https://www.markey.senate.gov/news/press-releases/senators-markey-merkley-lead-colleagues-on-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology (discussing the reintroduction of legislation to preclude government use of biometric technology, including FRT).

[145] *Id.*

[146] *See* Shannon Flynn, *13 Cities Where Police Are Banned from Using Facial Recognition Tech*, INNOVATION & TECH TODAY, https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech (discussing different cities' approach to banning law enforcement from utilizing facial recognition technology).

the particularity of facial recognition is required. Also, ex-ante evaluation should set accuracy standards and ensure that the database is diverse enough so accuracy would increase, and misidentifications might decrease. This step is critical to eliminate the discriminatory effect of facial recognition. As for the protection of people of all races, the regulations must ensure the software's safety to ensure that any data will be shared. For the United States, one single law will not be enough to address and resolve the problem of systemic racism. However, a law imposing the neutrality of facial recognition might be a step forward to limiting biases against people of color.

Finally, an international solution might be considered by States. Indeed, in a globalized world, the implementation of a regulation on facial recognition might constrain other states to act as well and respect their regulations. For instance, the GDPR has a broad scope of application since it does not apply only within the European Union, but also European citizens outside the European Union must be granted the same protection. Therefore, American websites, like the New York Times, must meet the requirements set forth by the GDPR. Indeed, an international framework will ensure equal protection and standards for individuals and companies. In that sense, similar regulations to what has been exposed should be considered by States. First, accuracy should be controlled. Without any accuracy standard, facial recognition will still perpetuate racial discrimination and the oppression of minorities. Moreover, "[g]lobal accuracy standards would increase competition among FRT companies, driving up the need for accuracy and bias free technology even further."[147] Additionally, an international independent third party should be instituted to examine the compliance of States to regulations and ensure human rights are not violated using facial recognition. However, it might be complicated today to get an international agreement on facial recognition, so it is likely not feasible.[148]

One solution relied on the roles of corporations. Companies now have considerable power in politics.[149] The lack of government

[147] Jacques, *supra* note 65, at 152.

[148] *See id.* at 153 ("While an international moratorium and subsequent regulation is the ideal solution, it does not seem likely this solution is feasible").

[149] *See* Stacey Vanek Smith & Cardiff Garcia, *Companies Get Political, The Indicator From Planet Money*, NPR, at 02:04 (Jan. 13, 2021), https://www.

responses might make companies, who have been calling for change since 2019, lead the way. In 2022, after receiving criticism from experts on their facial recognition, Microsoft called for regulations on the accuracy of facial recognition.[150] Microsoft announced that it planned to remove tools that predict a person's gender, age, and emotional state.[151] This is just one of the company's many pushes for tighter control of its artificial intelligence products.[152] While welcome, this measure should be adopted by all the companies creating facial recognition. Companies have the expertise and the resources to meet the need to tackle racial bias in facial recognition.[153] The push of big companies might help the instauration of guidelines among the industry to regulate the sector.[154] Indeed, that would further the competition between companies to ensure accuracy. Even if a regulation between companies might be a good start, States should adopt policies to regulate facial recognition and meet their international human rights obligations. Thus, States will have to act on facial recognition in one way or another.

npr.org/2021/01/13/956553990/companies-get-political (discussing the political sway of American corporations in American politics through immense donations to campaigns in hopes of influencing policy).

[150] *See* Kashmir Hill, *Microsoft Plans to Eliminate Face Analysis Tools in Push for 'Responsible AI'*, N.Y. TIMES (June 21, 2022), https://www.nytimes.com/2022/06/21/technology/microsoft-facial-recognition.html(highlighting efforts at Microsoft to tighten controls of artificial intelligence products so as to ensure they do not lead to a harmful impact on society).

[151] *Id.*

[152] *See id.* (describing additional measures Microsoft is taking, including new controls on its facial recognition feature and the need to apply for access with an accompanying explanation on how the technology is planned to be used).

[153] David Kaye, (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression) *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/41/35, ¶ 15 (May 28, 2019) (highlighting the circumstances and factors that render private companies so well-suited to leading the way towards a solution).

[154] *See* Jacques, *supra* note 65, at 154 ("FRT companies across the globe must work together to create ethical guidelines for FRT and promote human rights when nations cannot or will not. Companies must take responsibility for their impact on human rights violations.").

VI. CONCLUSION

Despite the widespread use of Facial Recognition Technology, there has not been much State oversight to control and prevent harm to people, especially people of color, who are particularly targeted by facial recognition used by law enforcement. Regulations are necessary to prevent human rights violations. The rights of people of color and all people in general must be protected from violation. Therefore, States must act to meet their human rights requirements.

*   *   *

*   *   *