We Don't All Look the Same: Police Use of Facial Recognition and the *Brady* Rule

Jaylla Brown*

TABLE OF CONTENTS

* J.D., May 2022, The George Washington University Law School. B.A. 2019, Political Science, Hampton University. While I cannot list every person that has helped me make this happen, I would like to specifically thank my mother, Susan Brown, for her support throughout this journey, and both my grandmothers Rev. Nancy A. Brown and Patricia Onakoya for instilling in me the importance of education, journalism, and advocacy.

I. INTRODUCTION

Julia and Rosie Williams, two sisters from Farmington Hills, Michigan, were two and five years old when they watched their father get wrongfully arrested in their front yard on January 9, 2020. The girls looked on in tears as they saw their father pull into their driveway and immediately be handcuffed by police. It would be thirty hours until the Williams sisters saw their father again. After a day of disappearance, he told his family that he was arrested because of a computer error.

Their father was brought downtown to the police station to be questioned by detectives in a small room. While in this room, the detectives showed him two grainy stills taken from surveillance footage and a picture of his previous driver's license. In response to him telling the detectives that the man in the pictures from the surveillance footage was not him, a detective responded, "I guess the computer got it wrong too?" The father took a picture from the surveillance footage, held it next to his face and said, "I hope you don't think all Black people look alike." Despite his protest, Mr. Williams was detained and later released on bail. Luckily, his case was dismissed at his arraignment hearing because there was a second witness who had not identified Mr. Williams as the defendant.

Notwithstanding the dismissal of Mr. Williams' case, his daughters still live with the trauma of seeing their father get arrested for a crime he did not commit based on flawed facial recognition technology. But what would have happened if her father had to go to trial? Would he have access to the evidence he needed to defend himself in court? How would his lawyer build a case without any knowledge of the system that misidentified her client? Would the prosecutor be kind enough to inform the defense of the role facial recognition played in convicting him?

All of these questions arise when police cannot identify who they saw perpetrating a crime, so they rely on facial recognition to help them identify an unknown face.[1] While investigating a crime, the police can photograph a suspect and then use facial recognition to search that image against a database of mugshots and driver's licenses to help them identify that suspect by name.[2]

The fallible nature of facial recognition makes it particularly dangerous when used by law enforcement. Police sometimes use this technology in a manner that can be likened to a "virtual line-up."[3] However in this line-up, a human does not point to the suspect, an algorithm does.[4]

Many factors can influence the accuracy of this line-up. Most algorithms require human operation, so the operator's competence and lack

1. CLARE GARVIE ET AL., CTR. ON PRIV. & TECHNOLOGY GEO. L., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA (2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf [https://perma.cc/V3CL-U35Z].
2. *Id.* at 11-12.
3. *Id.* at 1.
4. *Id.*

of bias are crucial.[5] Additionally, there are factors that affect the accuracy of the algorithm itself. Facial recognition algorithms have higher rates of misidentification for Native Americans, African Americans, and Asian Americans.[6] They also have higher error rates for identifying women in comparison to men.[7] The least accurate error rates are most commonly seen in subjects who are female, Black, and eighteen to thirty years old.[8] Facial recognition technology performs worst on darker-skinned females, with the highest rate of error at 34.7%.[9] The darker the skin, the more errors, and gender orientation makes algorithm accuracy even more difficult to achieve.[10]

Given the substantial risk of misidentification for women and Black people by facial recognition, defendants should be able to challenge these factors in order to argue that they have been falsely matched based on their race or gender. If the operation of a system or the algorithm itself is flawed, then the identification decision is flawed. If a defendant can produce evidence that exposes a faulty identification, they can argue that the system identified the wrong suspect. This is impossible if the defendant does not have access to that evidence. If the prosecution is aware of any materially exculpable evidence for the accused, there is a Constitutional obligation to disclose it.[11] But, if the prosecution fails to do so, the defense is handicapped.[12]

In *Brady v. Maryland*, the Supreme Court held that nondisclosure of exculpatory evidence to the defendant violates the Due Process Clause of the Fourteenth Amendment, which entitles defendants to the right to a fair trial.[13] Scholars have suggested the *Brady* rule poses a doctrinal solution for access to facial recognition evidence.[14] However, this Note focuses specifically on *Brady* as a solution for defendants who have been misidentified by the technology based on their race or gender. These defendants are most likely to be misidentified by facial recognition and pursued as suspects by law enforcement.[15] The purpose of this Note is to demonstrate how evidence of racial or gender disparities impacting the accuracy of facial recognition

5. Amici Curiae Brief of ACLU et al. in Support of Petitioner at 15-16, Lynch v. State, 2019 WL 3249799 (Fla. July 19, 2019) (No. SC19-298).

6. PATRICK GROTHER ET AL., NAT'L INST. OF STANDARDS & TECHNOLOGY, FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 7 (2019).

7. *Id.* at 2.

8. Alex Najibi, *Racial Discrimination in Face Recognition Technology*, HARV.: SCI. NEWS (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ [https://perma.cc/3WC6-PDYG].

9. JOY BUOLAMWINI & TIMNIT GEBRU, GENDER SHADES: INTERSECTIONAL ACCURACY DISPARITIES IN COMMERCIAL GENDER CLASSIFICATION 1 (Sorelle A. Friedler & Christo Wilson eds., 2018).

10. Steve Lohr, *Facial Recognition Is Accurate, if You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html [https://perma.cc/99YE-MXTB].

11. *See* Brady v. Maryland, 373 U.S. 83, 87 (1963).

12. *See* Elizabeth Napier Dewar, *A Fair Trial Remedy for* Brady *Violations*, 115 YALE L.J. 1450, 1452 (2006).

13. *See Brady*, 373 U.S. at 86.

14. *See* Rebecca Darin Goldberg, *You Can See My Face, Why Can't I? Facial Recognition and Brady*, COLUM. HUM. RTS. L. REV. ONLINE, Apr. 12, 2021.

15. *Id.* at 271-72.

technology qualifies as *Brady* material that the prosecution is obligated to disclose.

Despite defendants' need to access evidence about whether facial recognition was used in order to challenge its accuracy and to prevail on a misidentification defense, the Florida First District Court of Appeal ruled that defendants are not even entitled to view photos of other potential suspects identified by a facial recognition search that led to their arrest.[16] The court reasoned that because there is no reasonable probability the result of a trial would change if this evidence was disclosed to a defendant, there is no defendants' right to disclosure under *Brady*.[17] This opinion comes from *Lynch v. State*, where the court ultimately sentenced a Black man to eight years in jail for selling cocaine in 2016.[18] Lynch planned to use other photos that the facial recognition software produced alongside his to prove that he had been misidentified.[19] He argued that since the other matches were also potential suspects returned by the system, they would cast doubt on his identification as the defendant.[20] The court rejected Lynch's argument and he was never able to see the other photos produced by the system.[21]

The facial recognition system that identified Lynch, along with the pictures of four other potential suspects he was never able to see, is called the Face Analysis Comparison and Examination System (FACES).[22] Pinellas County Sheriff Department in Florida launched FACES in 2001, and since then it has become one of the most advanced statewide facial recognition systems in the country.[23] In 2020, the Department indicated that there were no plans of discontinuing the use of FACES despite the recent criticism that police use of facial recognition technology has received.[24]

This Note will explain why police use of facial recognition technology for criminal identification should be defined as exculpatory evidence that prosecutors have a duty to disclose under *Brady*. Part II, Section A will explain what facial recognition is and how it works. Section B will outline the racially discriminatory implications underlying facial recognition systems. Section C will discuss how law enforcement uses facial recognition. Section D will detail the *Lynch* case which illustrates how a Florida court has treated

16. *Lynch v. State*, 260 So. 3d 1166, 1169-70 (Fla. Dist. Ct. App. 2018).

17. *Id.*

18. Aaron Mak, *Facing Facts: A Case in Florida Demonstrates the Problems with Using Facial Recognition to Identify Suspects in Low-Stakes Crimes*, SLATE (Jan. 25, 2019, 12:49 PM), https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html [https://perma.cc/7XH3-MDXR].

19. *Id.*

20. Brief for Lynch at *17-18, *Lynch v. Florida*, No. 1D16-3290, 2017 WL 11618201 (Fla. App. 1 Dist. May 25, 2017).

21. *Lynch*, 260 So. 3d at 1170.

22. Amici Curiae Brief of ACLU et al., *supra* note 5, at 3.

23. Jerry Iannelli, *Miami-Dade Cops Want Permanent Access to Controversial Facial Recognition Database*, MIA. NEW TIMES (Nov. 8, 2019, 9:00 AM), https://www.miaminewtimes.com/news/miami-dade-police-department-wants-to-use-pinellas-county-faces-facial-recognition-database-11313634 [https://perma.cc/3AG5-24P8].

24. Malena Carollo, *Florida Police Embrace Facial Recognition Despite Pushback*, GOV'T TECHNOLOGY (June 26, 2020), https://www.govtech.com/public-safety/florida-police-embrace-facial-recognition-despite-pushback.html [https://perma.cc/C7TV-3YAP].

facial recognition as evidence in criminal court. Section E will explain what the *Brady* rule is. Part III will assert why facial recognition technology evidence qualifies as *Brady* material for minorities and women of color. Part III, Section A will explain why police misuse of facial recognition qualifies as *Brady* material for said defendants. Finally, Section B will explain why evidence of poor algorithm quality qualifies as *Brady* material.

II. BACKGROUND

A. What Is Facial Recognition?

Facial recognition is a form of biometrics that was created in the mid-1960s.[25] Biometrics is a technical term for body measurements and calculations such as DNA and fingerprints.[26] Biometrics is used to compare one piece of information to a dataset in order to determine someone's identity.[27] Where biometrics could involve a fingerprint analysis—comparing one fingerprint against a database of fingerprints to find a match—facial recognition aims to verify a person's identity by comparing a face against a dataset of other faces to produce a match.[28] The face that is compared to the dataset is called a probe image, which can be sourced from a photograph or video.[29]

Before the software can match someone's face to others in a given database, an algorithm is used to find the person's face within the reference image.[30] Then, the system reads the geometry of the face to determine key characteristics such as the distance between the eyes and the distance from the forehead to the chin.[31] Those characteristics make up a "facial signature" which is a mathematical formula that the system can understand.[32] After the facial signature is created, the system "normalizes" the face by scaling, rotating and aligning it to optimize positioning for comparison to the dataset of other faces.[33] Lastly, the algorithm examines pairs of faces and assigns a numerical score that reflects the similarity of the matches.[34]

---

25. CRIMINAL CTS. COMM., N.Y.C. BAR ASS'N, POWER, PERVASIVENESS AND POTENTIAL: THE BRAVE NEW WORLD OF FACIAL RECOGNITION THROUGH A CRIMINAL LAW LENS (AND BEYOND) 1 (2020).

26. *Id.*

27. *Id.*

28. *Street-Level Surveillance: Face Recognition*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/face-recognition [https://perma.cc/AZP9-FRB7].

29. Kaitlin Jackson, *Challenging Facial Recognition Software in Criminal Court*, CHAMPION, July 2019, at 14.

30. GARVIE ET AL., *supra* note 1, at 9.

31. Steve Symanovich, *What Is Facial Recognition? How Facial Recognition Works*, NORTON (Aug. 20, 2021), https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html#:~:text=Facial%20recognition%20software%20reads%20the,The%20result%3A%20your%20facial%20signature. [https://perma.cc/9PMA-53QT].

32. *Id.*

33. GARVIE ET AL., *supra* note 1, at 9.

34. *Id.*

The algorithm that examines and compares the probe image to the faces in a database is a machine learning system.[35]A machine learning system must be trained to examine and analyze faces. The data used to train an algorithm is called a "training data set" comprised of faces that help the system practice identifying facial characteristics for comparison.[36] But the demographics of that training set strongly influence the algorithm's ability to accurately interpret a diversity of faces.[37] For example, "if a training set is skewed towards a certain race, the algorithm may be better at identifying members of that group as compared to individuals of other races."[38] This concept is known as "overfitting" to the training data.[39]

Facial recognition algorithms tend to be probabilistic in nature.[40] They do not produce a binary "yes or no" answer, but instead identify more likely to less likely matches.[41] This type of algorithm is referred to as a "one-to-many" search algorithm because it compares the facial signature from a probe image to all the facial features found in the faces from the dataset.[42] Once each match has been assigned a numerical value or "score" that reflects the level of similarity, that value is compared against a threshold value that helps the system determine whether the two faces represent the same person.[43] The threshold value, set by algorithm developers, determines how high the match score must be to signify that the two images are of the same person.[44] The key components that affect the accuracy of facial recognition software fall into two categories: (1) the operation of the system, and, (2) the development of the algorithm. Each of these can be problematic.

B. Problems with Facial Recognition

1. Operational Flaws

Like any other technology or system, the success and accuracy of it largely depends on how well it is being operated. "Since face recognition accuracy remains far from perfect, experts agree that a human must double-check the results of face recognition searches to ensure that they are correct."[45] It follows that the more skilled the human reviewer, the more accurate the search is.[46] But issues arise when the human reviewer is not

35. *See* P'SHIP ON AI, UNDERSTANDING FACIAL RECOGNITION SYSTEMS 4 (2020).
36. Alexandre Gonfalonieri, *How to Build a Data Set for Your Machine Learning Project*, TOWARDS DATA SCI. (Feb. 13, 2019), https://towardsdatascience.com/how-to-build-a-data-set-for-your-machine-learning-project-5b3b871881ac [https://perma.cc/A8L4-QSPT].
37. GARVIE ET AL., *supra* note 1, at 9.
38. *Id.*
39. *See* Daniel Nelson, *What Is Overfitting?*, UNITE.AI (Aug. 23, 2020), https://www.unite.ai/what-is-overfitting/ [https://perma.cc/RQ6G-HJPY].
40. GARVIE ET AL., *supra* note 1, at 9.
41. *Id.*
42. *See* GROTHER ET AL., *supra* note 6, at 5.
43. *See id.* at 4.
44. P'SHIP ON AI, *supra* note 35, at 6.
45. GARVIE ET AL., *supra* note 1, at 49.
46. *Id.*

knowledgeable on how the facial recognition technology works or how it has a substandard ability to recognize faces.[47] Adequate operational training greatly impacts the success of a facial recognition program because it helps to avoid human errors that stem from implicit bias, lack of expertise, or incompetence. However, the lack of uniform operational standards for the people using facial recognition fails to hold entities accountable to provide effective training.[48]

a. Human Review Bias

Human reviewers are susceptible to biases that can negatively impact their ability to check the results produced by an algorithm depending on what information the software gives them. Some state forensic scientists may feel pressure to interpret results in a way that is favorable to the state government pushing for a conviction.[49] Some facial recognition systems, such as Florida's FACES, show candidates' criminal history alongside the results that are matched to a probe image.[50] If a facial recognition search returns multiple possible matches for a suspect along with the criminal history of each suspect, the analyst may be biased against the person with the longest or most severe history, and, thus, more likely to confirm that person as the actual match. A study on a subjectivity and bias when operating DNA analysis, a different but comparable forensic tool to facial recognition, found that forensic DNA analysts were influenced and possibly biased by extraneous information concerning the DNA they examined.[51] Developers of facial recognition systems must account for these risks when training their operators.

Along with the risk of human reviewers being influenced by tangential information, there are also psychological biases that can impact a person's neutrality when reviewing potential matches. According to an experiment conducted in 2015, researchers found that people are better at making judgements about face pairings with faces that they know rather than those they do not.[52] Not only are unfamiliar faces harder for humans to recognize, but evidence shows that people are generally better at recognizing those from their same race, which creates dire risks for people of color.[53]

In-depth training for human reviewers could address implicit bias concerns when operating facial recognition. One study tested the accuracy of Australian passport personnel after using an algorithm to check for duplicate passport applications.[54] The personnel who receive limited instruction in face

47. *Id.*
48. Goldberg, *supra* note 14, at 270.
49. Amici Curiae Brief of ACLU et al., *supra* note 5, at 3.
50. *Id.* at 16 (arguing that analysts' bias may be exacerbated when they are aware of the identified individual's criminal history when interpreting the results of a facial recognition search).
51. *Id.* (citing Itiel E. Dror & Greg Hampikian, Subjectivity and Bias in Forensic DNA Mixture Interpretation, 51 SCI. & JUST. 204, 205–07 (2011)).
52. Kay L. Ritchie et al., *Viewers Base Estimates of Face Matching Accuracy on Their Own Familiarity: Explaining the Photo-ID Paradox*, 141 COGNITION 161 (2015).
53. GARVIE ET AL., *supra* note 1, at 49.
54. *Id.*

matching were only accurate fifty percent of the time compared to the trained facial examiners who outperformed them by twenty percent .[55] Despite the benefits that human training can have, not all facial recognition systems train their operators the same.

b. Poor Personnel Training

There are some private companies and entities that employ operational guidelines for their facial recognition technology, but there is no national standard for how these analysts should be trained for reviewing results.[56] A lack of uniformity in training and operations oversight leaves room for varied efforts by human operators to ensure that the results produced by facial recognition systems are accurate. One facial recognition search conducted by Detroit police yielded six possible suspect matches, which were then shown to a security guard who never saw the person in question but was tasked with confirming the correct match for identification.[57] In that instance, the only human review on the facial recognition results was an untrained outside individual. Some facial recognition searches evade human review altogether when police conduct facial recognition searches in the field with their mobile devices, and the algorithm produces instantaneous results.[58] Until the personnel operating facial recognition systems are held to a uniform standard, the risk for human error remains one of the biggest operational flaws to which the technology is susceptible.

2. Algorithmic Flaws

Facial recognition systems vary in their ability to identify people, and no system is 100% accurate.[59] Most facial recognition systems are built using algorithms to detect faces,[60] which is a crucial part of the system. Algorithm accuracy is influenced by the quality of the probe image being searched, the enrollment database the image is compared to, the training set database the algorithm is developed with, and the match thresholds set by developers.[61] All these factors influence the algorithm's ability to accurately return matches in a search, and conditions like race, sex, and gender are an added layer that

55. *Id.*

56. CRIMINAL CTS. COMM., *supra* note 25, at 21.

57. Letter from Phil Mayor, Senior Staff Att'y, ACLU Fund of Michigan, to Chief Investigator, Detroit Pub. Safety Headquarters (June 24, 2020). This is referring to an incident of false identification of Robert Williams by Detroit Police Department when they used facial recognition and will be discussed later in Part II, Section C. How Law Enforcement Uses Facial Recognition.

58. GARVIE ET AL., *supra* note 1, at 50.

59. JENNIFER LYNCH, ELEC. FRONTIER FOUND., FACE OFF: LAW ENFORCEMENT USE OF FACE RECOGNITION TECHNOLOGY 6 (Gennie Gebhart ed., 2019).

60. Thorin Klosowski, *Facial Recognition Is Everywhere. Here's What We Can Do About It.*, N.Y. TIMES: WIRECUTTER (July 15, 2020), https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/ [https://perma.cc/4WY6-TCY7].

61. P'SHIP ON AI, *supra* note 35, at 4.

complicates developing the best algorithm to identify individuals with precision.

a. Probe Image Quality

As previously mentioned, most one-to-one facial recognition systems require a probe image as a basis for comparison to find a match within a database.[62] The quality of a probe image heavily influences the system's ability to return an accurate match.[63] If the probe image is at a low resolution, it is more difficult for the algorithm to decipher the facial signature of the probe at the stage before comparison.[64] Factors such as angle lighting and the newness of the technology used to capture the image all impact the quality of the probe image.[65] All of these variables should be taken into consideration when evaluating the risk of error caused by a low quality probe image used in a facial recognition search.

b. The Enrollment Database

The quality of the enrollment database that the probe image is compared against is also important to the overall accuracy of the algorithm. Problems arise when this database is not adequately representative of the population that the facial recognition technology is being used on. "Law enforcement search their probe images against a database of mug shots, driver's licenses, or . . . unsolved photo file[s]," so these are the sources for their enrollment database.[66] However, the issue of racial bias arises because "years of well-documented racially biased police practices" have resulted in a disproportionate number of African Americans, Latinos, and immigrants included in criminal databases.[67] San Francisco is a prime example of the racial implications resulting from the over-policing of Black communities. "Over-policing" is defined as strategic police practices in which studies show that when police increase their presence in Black communities, there is an increased likelihood of disproportionate levels of stops, searches, arrests, and pretrial detention for Black people.[68] "African American women make up only 5.8% of San Francisco's total female population, but constituted 45.5% of all female arrests in 2013."[69] The overrepresentation of minorities, especially African Americans, in mugshot enrollment databases means that

62. Jackson, *supra* note 29, at 14.
63. Amici Curiae Brief of ACLU et al., *supra* note 5, at 5.
64. *Id.* at 5-6.
65. *Id.* at 6.
66. GARVIE ET AL., *supra* note 1, at 11.
67. *Id.* at 57 (citing NAACP, Criminal Justice Fact Sheet (2009) ("A Black person is five times more likely to be stopped without just cause than a white person . . . 32% of the US population is represented by African Americans and Hispanic, compared to 56% of the US incarcerated population being represented by African Americans and Hispanics").
68. *See* ELIZABETH HINTON ET AL., AN UNJUST BURDEN: THE DISPARATE TREATMENT OF BLACK AMERICANS IN THE CRIMINAL JUSTICE SYSTEM 2 (2018).
69. GARVIE ET AL., *supra* note 1, at 56.

they are statistically more likely to be matched to a probe image when it is searched against an overwhelming number of Black faces.

In a study that examined the accuracy of a facial recognition software created by Amazon, the system misidentified twenty-eight members of Congress who were overwhelmingly people of color.[70]Amazon's "Rekognition" face recognition software used 25,000 publicly available arrest photos which resulted in false-positive matches for six members of the Congressional Black Caucus.[71] Among those members was the late "civil rights legend," John Lewis.[72] The *New York Times* labeled him a "towering figure of the Civil Rights Era" who "led one of the most famous marches in American history."[73] However, his longtime recognition on the national political stage had no bearing on the software that identified his face as a match to a convicted criminal. The test done on "Rekognition" revealed the shortcomings of facial recognition algorithms as opposed to the likelihood of a person identifying the face of an easily well-known political figure.

c. The Training Database

The alternative to mugshot enrollment databases also inadequately addresses the problem of racial bias. Most developers for facial recognition algorithms only have access to an open-source collection of images because of the time and cost required to create their own dataset.[74] The disadvantage of using open-source collections is that they are often limited in diversity.[75] A popular open-source dataset named "Labeled Faces in the Wild" was estimated to be comprised of 77.5% males and 83.5% white people.[76] When developers use open-source datasets like these, the algorithm quality is diminished because that dataset is not representative of real-world conditions that would encompass a diverse plethora of faces that the system would need to understand how to match.[77]

Lack of diversity in training sets that are used during the developing stages of facial recognition algorithms create a higher risk for overfitting. Overfitting is essentially "built-in racial bias."[78] An NIST study found that more diverse training data can be effective at reducing false positives.[79]

---

70. Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (July 26, 2018, 8:00 AM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [https://perma.cc/EGC4-7TKR].

71. *Id.*

72. *Id.*

73. Katharine Q. Seelye, *John Lewis, Towering Figure of Civil Rights Era, Dies at 80*, N.Y. TIMES (Aug. 4, 2020), https://www.nytimes.com/2020/07/17/us/john-lewis-dead.html [https://perma.cc/RA6T-KSUT].

74. Open Data Science, *The Impact of Racial Bias in Facial Recognition Software*, MEDIUM (Oct. 15, 2018), https://medium.com/@ODSC/the-impact-of-racial-bias-in-facial-recognition-software-36f37113604c [https://perma.cc/9Y7N-DHDV].

75. *Id.*

76. *Id.*

77. *Id.*

78. *Id.*

79. GROTHER ET AL., *supra* note 6, at 71.

Conversely, the study found that false positives and false negatives likely resulted from a lack of demographic diversity in training data.[80] A "false positive" means that the algorithm matches the probe photo to an image in the database, but the match is incorrect.[81] A "false negative" is when the algorithm fails to match the probe image to an image that is, in fact, contained in the database.[82] Both of these errors should be avoided in facial recognition.

On the one hand, a criminal database mostly comprised of Black faces is problematic because it could lead to false positive matches disproportionate to the number of Black people in the system. Conversely, when an overwhelmingly white male database is used to train the algorithm, it makes it more difficult for the algorithm to accurately examine and match non-white people which also leads to false positives and negatives. In sum, the database that an image is being searched against must be diverse, but not overly representative of any one race or gender, and the database used to train the algorithm to work must be diverse enough so that it has the capacity to accurately examine a probe image regardless of race or gender.

d. The Match Threshold

Match thresholds are another variable that can impact algorithm accuracy in facial recognition. As previously mentioned, match thresholds are set values against which the algorithm compares its match score to determine if it has found a match to the probe image. The higher the match threshold, the fewer results produced, which garners a stronger possibility that the actual match will be missed by the system (creating a false negative).[83] On the other hand, the lower the threshold value, the more results produced (meaning a higher chance for false positives).[84] The threshold value has a significant impact on facial recognition results and therefore has the potential to create issues where the search should be more stringent or in instances where the goal of the search is to cast a wide net.[85] This algorithm component works in tandem with the skill of the analyst because a wider range of results would require more judgement from the person operating the system, while a narrower search return causes the analyst to rely more heavily on the algorithm accuracy as opposed to their own judgement.

e. Algorithm Accuracy for Intersectional Demographics

Numerous studies have been performed which reflect the low accuracy rates in facial recognition algorithms based on race, gender, age, and sexual orientation. An MIT researcher conducted an intersectional demographic and

80. *Id.*
81. Amici Curiae Brief of ACLU et al., *supra* note 5, at 6 n. 15.
82. *Id.*
83. P'SHIP ON AI, *supra* note 35, at 6.
84. *Id.*
85. *Id.* at 7.

phenotypic analysis on facial recognition algorithm accuracy.[86] The study classified subjects by phenotypic subgroup (dark-skinned females, light-skinned females, light-skinned males, and dark-skinned males) in order to test algorithm accuracy of race and gender classification simultaneously.[87] Because people have multiple identities that intersect and are not exclusive, such as white women or transgender Black men, it was important to test how algorithms perform when categorizing faces belonging to multiple classifications. Given the poor accuracy for algorithms when identifying Black people and women generally, it made sense that the poorest algorithmic accuracy was seen in dark-skinned women.[88] This study reflects the nuanced disparity in facial recognition among members of the same race.

C. Problems with Law Enforcement Use of Facial Recognition

Law enforcement mainly uses facial recognition for one of two purposes, facial verification or facial identification, the latter of which is most relevant for purposes of this Note.[89] Police use facial identification to identify unknown people in photos and videos.[90] Facial identification is used as an investigative tool by law enforcement.[91] Facial recognition is used to help police narrow leads on suspects, and once a suspect is identified, law enforcement and prosecution gather other incriminating evidence against that person to be used in court and in charging documents.[92] The inherent issue with using facial recognition during the investigative process is that it can be concealed because the police have no legal duty to disclose information about their investigations, and the prosecution only has to disclose what they plan to use for trial.[93]

Given all the factors that impact the accuracy of facial recognition, the biggest problem with law enforcement using it during investigation lies in the risk that police could misidentify a suspect during their investigation which then taints the entire case going forward. Although the police should further investigate a lead chosen by facial recognition, there is a concern that law enforcement relies too heavily on the technology to get an arrest. Because of a lack of standards for facial recognition and a lack of transparency surrounding its use in police departments, the risk for misidentification is high when police rely too heavily on this technology and no uniform standards exist to prevent its misuse.

86. BUOLAMWINI, *supra* note 9, at 10.
87. *Id.*
88. *See id.*
89. GARVIE ET AL., *supra* note 1, at 10.
90. *Id.*
91. Jackson, *supra* note 29, at 16.
92. *Id.*
93. *Id.*

The individuals who have been falsely arrested based on a bad facial recognition match focused on in this Note are all Black men.[94] The common thread throughout their cases were the steps that police took, or did not take, directly after facial recognition systems produced their pictures as matches to a suspect. These scenarios highlight the problematic nature of police use of facial recognition and how the veil of the investigatory stage insulates police departments from accountability.

The false arrest of Robert Julian-Borchak Williams is a perfect example of the faulty investigatory steps that police take when relying on equally faulty facial recognition technology. In October 2018, the Detroit Police Department (DPD), began an investigation into a store robbery committed by an unidentified Black man captured on surveillance footage.[95] Five months later, DPD ran the suspect's image through a facial recognition software which returned Williams as a match to the suspect.[96] Four months later, DPD showed a picture of Williams alongside five other pictures to a security guard who worked at the site of the robbery, and did not witness the robbery itself, but watched the surveillance footage from that day.[97] On the basis of this security guard's identification of Williams, DPD obtained an arrest warrant for him.[98] Six months later, DPD called Williams and told him to report to the station to surrender. When Williams refused to do so, DPD showed up at his house and arrested him.[99] He was interrogated and held for thirty hours until he was released on bail. Ultimately, the prosecutor dropped all charges at the probable cause hearing due to "insufficient evidence".[100] According to NPR, the use of facial recognition technology was disclosed on Williams' charging documents, so his lawyer had asserted that the system had falsely identified him.[101]

Another victim of facial recognition misidentification is Nijeer Parks, who was accused of shoplifting candy and trying to hit a police officer with a car in February 2019.[102] Much like the officers in the *Lynch* case, described in the following section of this Note, the police were unable to identify the man who they saw commit the crime when it occurred, so they sent a reference photo from the ID they retrieved at the scene to search using facial recognition software.[103] After the system produced Mr. Parks as a match, the officers

94. *See generally* Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Jan. 6, 2021), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html [https://perma.cc/Y9UA-QZ76]; Mak, *supra* note 18.

95. Mayor, *supra* note 57.

96. *Id.*

97. *Id.* The security guard was not present at the armed robbery but was presented with the footage by police to help confirm the suspect that the facial recognition software had matched with the person in the video.

98. *Id.*

99. *Id.*

100. *Id.*

101. *Id.*

102. Hill, *supra* note 94.

103. *Id.*

obtained a warrant.[104] When Parks' grandmother told him there was a warrant out for his arrest, he called the police station to clear up the mistake, but when he arrived, officers interrogated and arrested him.[105] Parks sat in jail for ten days while police failed to check for DNA or fingerprints to confirm that he was at the scene of the crime.[106] Swayed by his fear of the criminal justice system, Parks almost took a plea deal despite his innocence.[107] Parks' case was dismissed four months after his last hearing because he obtained proof that he was more than thirty miles away when the crime occurred.[108]

When comparing the incidents of facial recognition misidentification by police departments, there is a common theme of overconfidence in the results produced by these algorithms. Both the Detroit and New Jersey police departments employed limited checks before hotly pursuing the false matches of their searches. Neither of the cases went to trial, so most of the scrutiny rests on law enforcement's poor investigatory decisions and the part that they played in the false arrests of two Black men based on algorithm error. But, if these types of cases do go to trial, the next important question is whether courts will consider evidence of faulty facial recognition technology used during police investigations as "exculpatory" within the context *Brady*? This issue was brought to light for the first time when a defendant challenged the evidentiary standards for facial recognition in court, in *Lynch v. Florida*.[109]

D. Facial Recognition in Courts: Lynch v. Florida

On September 12, 2015, undercover officers bought cocaine from someone who called himself "Midnight."[110] One of the officers "used his cellphone to surreptitiously snap photos of Midnight during the transaction."[111] The officers sent the cell phone pictures, the name Midnight, and the address where the crime occurred to a crime analyst to find a name that matched the photos they had taken.[112] Sixteen days after the officers purchased the cocaine from Midnight, they received notification from the crime analyst of a match to the picture they sent.[113] The analyst testified that the program allowed her to filter the race and gender of the search to which

104. *Id.*

105. Elura Nanos, *Third Innocent Black Man to Be Misidentified by Facial Recognition Software Sues Police Department and Prosecutor for False Arrest and Imprisonment*, LAW & CRIME (Dec. 31, 2020), https://lawandcrime.com/civil-rights/third-innocent-black-man-to-be-misidentified-by-facial-recognition-software-sues-police-department-and-prosecutor-for-false-arrest-and-imprisonment/ [https://perma.cc/GNU3-7Z36].

106. *Id.*

107. *Id.*

108. Hill, *supra* note 94.

109. *See* Lynch v. State, 260 So. 3d 1166, 1170 (Fla. Dist. Ct. App. 2018).

110. Benjamin Conarck, *How a Jacksonville Man Caught in The Drug War Exposed Details of Police Facial Recognition*, FLA.-TIMES UNION (May 26, 2017, 11:00 AM), https://www.jacksonville.com/news/metro/public-safety/2017-05-26/how-jacksonville-man-caught-drug-war-exposed-details-police [https://perma.cc/93PY-CYHS].

111. *Lynch*, 260 So. 3d at 1168-69.

112. *Id.*

113. *See* Appellant's Motion for Rehearing and Written Opinion at 7, Lynch v. State, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018) (No. 1D16-3290).

she input "Black male," and also narrowed the search to "Duval County booking photos".[114] That match was to a man named Willie Allen Lynch, who was later arrested for selling cocaine.[115]

At the pre-trial hearing, the crime analyst testified that she used the facial recognition program, FACES, to compare the photo of Midnight against other photos in a law enforcement database.[116] The analyst explained that the software would assign a number of stars indicating the likelihood of a match.[117] There were also other photos that the system returned as possible matches, but she only sent the officers a picture of Lynch along with his criminal history.[118] She admitted that she did not know how many stars were possible or what the number of stars meant, but that Lynch's photograph only had one star next to it.[119] Lynch did not learn that facial recognition was used to identify him until months after the trial began; this was during deposition of the investigators, as it was not mentioned in his arrest report.[120] The defendant filed a motion seeking to compel the State to produce the other photos that FACES returned—to which the court denied.[121] The court convicted Lynch and he was sentenced to eight years in prison.[122]

On appeal, Lynch argued that he should have had access to the other photos that FACES returned because they would have cast doubt on the State's case.[123] He contended that by not providing these photos, the State violated *Brady v. Maryland*.[124] The appellate court rejected this argument on the basis that Lynch failed to show that "there is a reasonable probability that the result of the trial would have been different if the suppressed documents had been disclosed to the defense."[125] The court reasoned that because his sole defense was misidentification, and the police wholly relied on the facial recognition system to identify him as "Midnight," he would need the other pictures to show he was not the suspect.[126] Lynch presented other arguments which were all rejected, and, subsequently, the trial court decision was affirmed.[127]

E. What Is the Brady Rule?

In *Brady*, the Supreme Court held that suppression of evidence favorable to the accused amounts to the denial of due process.[128] Under the

114. *Id.* at 3.
115. *Lynch*, 260 So. 3d at 1169.
116. *Id.*
117. *Id.*
118. *Id.* at 1170.
119. *Id.*
120. Mak, *supra* note 18.
121. *See Lynch*, 260 So. 3d at 1169.
122. *Id.* at 1168.
123. *Id.* at 1169-70.
124. Brady v. Maryland, 373 U.S. 83, 87 (1963).
125. *See Lynch*, 260 So. 3d at 1170.
126. *Id.*
127. *Id.* at 1172.
128. *Brady*, 83 U.S. at 87.

Due Process Clause of the Constitution, the prosecution has a duty of disclosure if failing to do so would deprive the defendant of his right to a fair trial.[129] Although the Supreme Court has never classified facial recognition evidence as *Brady* material, many of the Court's decisions about the *Brady* doctrine create a framework to draw comparisons between traditional *Brady* material and facial recognition technology.[130]

In *Brady*, the Court held that the suppression of evidence favorable to an accused upon request violates due process where the evidence is "material either to guilt or punishment."[131] In that case, the petitioner was convicted of murder, but the State withheld a statement in which another individual admitted to committing the homicide.[132] While the Supreme Court noted that there was doubt in considering how much good the undisclosed confession would have done the defendant, the Court ultimately concluded that withholding the statement was prejudicial to the defendant, and, therefore, his due process rights were violated.[133]

The *Brady* Court sets forth a two-part test for whether the State is required to turn over evidence. The evidence in question must be (1) favorable to the defense and (2) material to the defendant's guilt or punishment.[134] Evidence is "material" when there is a "reasonable probability" that, if disclosed, the result of the proceeding would have been different.[135] A showing of materiality does not require demonstration by a preponderance of the evidence that disclosure of the suppressed evidence would have resulted ultimately in an acquittal.[136] Rather, the touchstone of materiality is whether in the absence of the evidence, the defendant has received a fair trial.[137] "*Brady* material" is defined as evidence that is materially exculpatory.[138] This means that the government's evidentiary suppression has undermined confidence in the outcome of the trial.[139]

"When the reliability of a given witness may well be determinative of guilt or innocence," nondisclosure of evidence affecting credibility falls within this general rule.[140] This principle, articulated in *Giglio*, represents the idea that evidence that impeaches a witness may constitute *Brady* material because it casts doubt on the guilt of a given defendant. Evidence that casts doubt on the reliability of the State's case against a defendant is "favorable" to the defense.

The *Kyles* case is instructive in determining whether a defendant has satisfied the materiality prong of the *Brady* test. In *Kyles*, the defendant was

129. United States v. Agurs, 427 U.S. 97, 108 (1976).

130. *See generally Brady*, 83 U.S. at 87; Giglio v. United States, 405 U.S. 150, 154 (1972); Kyles v. Whitley, 514 U.S. 419, 434 (1995).

131. *Brady*, 83 U.S. at 87.

132. *Id.* at 84.

133. *Id.* at 88.

134. *Id.* at 87.

135. United States v. Bagley, 473 U.S. 667, 682 (1985).

136. Kyles v. Whitley, 514 U.S. 419, 434 (1995).

137. *Id.*

138. *Id.*

139. *Id.*

140. Giglio v. United States, 405 U.S. 150, 154 (1972) (internal citation omitted).

tried and convicted of first-degree murder.[141] The Court found that the net effect of the evidence suppressed by the State amounts to a reasonable probability that its disclosure would have produced a different result.[142] Put differently, in answering the question of materiality, the Court considers all favorable evidence collectively, not separately. In *Kyles*, the Court held that the prosecutor was required to disclose evidence that the police ignored during their investigation because that evidence served to exculpate the defendant.[143]

III. FACIAL RECOGNITION EVIDENCE IS *BRADY* MATERIAL FOR A MISIDENTIFICATION DEFENSE

Evidence of police misuse of facial recognition and poor algorithm quality is *Brady* material for defendants alleging misidentification based on race or gender. For evidence to be classified as *Brady* material, the defendant must show that the evidence is both favorable and material.[144] To avoid the fundamental unfairness of police reliance on facial recognition technology that impacts racially vulnerable defendants, under the *Brady* rule, courts should require the prosecution to disclose its use. Once defendants are aware that facial recognition was used by police leading up to their arrest, there are two types of facial recognition evidence that warrants disclosure under *Brady*. Part III, Section A will show how evidence of faulty operation tactics committed by police using facial recognition qualifies as *Brady* material. Section B will describe how evidence of poor algorithm quality in facial recognition used by the police meets the *Brady* evidentiary standard.

A. Evidence of Poor Operating Choices Taken by Police Departments when Using Facial Recognition Qualifies as Brady Material

The previously mentioned incidents of Mr. Williams, Mr. Parks, and Mr. Lynch all illustrate real-world examples of what can go wrong at each stage of investigation, and later at trial, when facial recognition is involved. Most of these problems arose because there is no uniform standard for how police departments and analysts should use facial recognition technology to avoid issues that prove detrimental to the people they police.

1. Evidence Indicating Poor "Human Review"

The central issue with how police departments operate their facial recognition technology is a lack of training for the person reviewing the

141. *Id.* at 421.

142. *Id.* at 421-22.

143. *See generally* Kyles v. Whitley, 514 U.S. 419, 446-48 (1995) (the police ignored a tip that the defendant had been framed, they disregarded evidence that supported this theory and the prosecution never disclosed this information to the defendant).

144. *See generally* Brady v. Maryland, 373 U.S. 83, 87 (1963).

algorithm results or a complete absence of human review at all. Any evidence that demonstrates inadequate training for the person that reviewed the results of a facial recognition search is material and favorable to the defendant and is thus *Brady* material.

Evidence of poor personnel training is material to a misidentification defense because it is a crucial factor tied to the reliability of a facial recognition search. The reliability of facial recognition search results is comparable to the credibility of a witness called to identify a defendant in court. If there is evidence that undermines a witness' credibility whose testimony the government solely relies on for their case, that witness' credibility becomes an important issue of the case as a whole.[145] Like in *Lynch*, the prosecution and police based their identification of the defendant solely on his match that was produced by FACES and thus any evidence undermining the reliability of that match is a material issue of his case.

Along with being material, the evidence must also be favorable to the defendant to satisfy *Brady*.[146] An example of favorable evidence concerning poor personnel training was when the crime analyst in *Lynch v. Florida* admitted to not knowing how to interpret the results presented by the facial recognition software used to identify Lynch.[147] The analyst's lack of understanding the system indicates that she was never properly trained to evaluate the algorithm and account for possible error. A government study stated that when the operator of a facial recognition software has some personal qualification for facial identification, the system is more likely to lead to accurate results.[148] But if an analyst has no personal qualification to operate a system, it tends to undermine the quality of the results produced by that system and thus bolsters the case for misidentification. Poor personnel training is both material and favorable to a misidentification defense, and thus should qualify as *Brady* material.

2. Evidence of Police Overreliance on Facial Recognition Technology

Police misconduct during the investigation is favorable for the defendant. In *Kyles*, the police ignored a tip that the defendant had been framed, they disregarded evidence that supported this theory, and the prosecution never disclosed this information to the defendant.[149] Similarly, in the false arrest of Nijeer Parks based on a bad facial recognition search, the

145. *Giglio*, 405 U.S. at 154-55 ("the Government's case depended almost entirely on Taliento's testimony; without it there could have been no indictment and no evidence to carry the case to the jury. Taliento's credibility as a witness was therefore an important issue in the case").

146. *See Brady*, 83 U.S. at 87.

147. Amici Curiae Brief of ACLU et al., *supra* note 5, at 20.

148. *See* P. Jonathon Phillips et al., *Face Recognition Accuracy of Forensic Examiners, Superrecognizers, and Face Recognition Algorithms*, 115 PROC. NAT'L ACAD. SCI'S. 6172 (June 12, 2018), https://www.pnas.org/content/pnas/115/24/6171.full.pdf [https://perma.cc/FXH2-4VVY].

149. *See* Kyles v. Whitley, 514 U.S. 419, 420 (1995).

police skipped vital steps in the investigatory process, leading to the detention of Mr. Parks. The police obtained a search warrant, interrogated, and jailed Parks for ten days without taking any further precautions to confirm that he was the correct suspect. The culmination of evidence showing a lack of diligence taken by the police, coupled with overreliance on one fallible identification is much like the faulty investigation described in *Kyles*. Under *Brady*, the court evaluates the net value of favorable evidence to the defendant and decides whether its disclosure would have undermined the outcome of the case.[150] If Parks' case would have gone to trial, the evidence describing the lack of diligence taken by the police after obtaining a false match would have been both material and favorable to his defense.

B. Evidence of Poor Algorithmic Quality Constitutes Brady Material

Prosecutors should be required to disclose the use of facial recognition as *Brady* material where the system was the only identification mechanism the witness relied on to identify a suspect. When facial recognition technology has matched a Black, brown, or female defendant, it may be enough to satisfy both the "material" and "favorable" *Brady* elements. Given the aforementioned empirical evidence that facial recognition systems are disproportionately unreliable at identifying minorities and women, those defendants are entitled to access information about the algorithm used to identify them, especially when it is the only evidence on which the government and police relied.

Usually only the police and prosecution know when facial recognition technology has been used to identify a defendant.[151] This fact is especially problematic when a match by a facial recognition software is the sole basis on which the police rest their identification; if the algorithm was flawed, the defendant has no way of knowing why they were identified. Further, the defendant then has no way of challenging it in court with evidence unless it has been disclosed under *Brady*.

1. The Name of the Algorithm

The name of the algorithm used to identify a defendant is the first step in the discovery process that attorneys must take in order to reveal algorithmic flaws made in the development of the facial recognition software. Although the company name alone is not likely to be exculpatory to the defendant, it is the first piece of evidence necessary for a misidentification defense to cast doubt on the quality of the facial recognition technology used. Without the name of the company, an attorney may not be able to find any more evidence informing the quality of the technology.

150. *Brady*, 83 U.S. at 87.
151. Jackson, *supra* note 29, at 16.

The facial recognition error rates of companies such as Microsoft, Facebook and IBM have been published in academic studies.[152] If the name of the algorithm is disclosed, the defense could present evidence about that system to cast doubt on its accuracy towards people of color and women. If the defendant falls within a class of regularly misidentified people by that algorithm, this evidence would be "material to either guilt or punishment."[153] For example, if a Black defendant has been identified using "Amazon Rekognition," evidence of that company's history of misidentification of people of color would lead to a "reasonable probability" that the algorithm results may be wrong. This is the touchstone for *Brady* material.[154]

2. Other Matches Produced by the Algorithm

The other matches returned in a search is evidence that qualifies as *Brady* material. The other matches produced by an algorithm are exculpatory in nature because they cast doubt on the identification of the defendant as the suspect. When there are other possible suspects to a crime, the existence of those suspects serves to cast doubt on whether the defendant was correctly identified.[155] This can be likened to *Kyles*, where the government suppressed evidence of other suspects which may have changed the outcome of the case had they been admitted into evidence.[156]

The presence of other matches in the system works to contradict the reliability of the witness that identified the defendant. The admission of contradictory evidence satisfies the impeachment requirement of evidence that would constitute *Brady* material. Contradictory evidence would likely change the outcome of the case, and, thus, satisfies the "reasonable probability" prong for *Brady* evidence.

3. The Confidence Scores of Other Matches Produced

The confidence scores of the other matches should constitute *Brady* material if the scores are high because they could cast doubt on the positive identification of the defendant.[157] High confidence scores for other suspects that were ignored by police in the identification process undercuts the quality of the investigation that was conducted in identifying the defendant. If the defendant shapes their argument around misidentification, evidence that informs the method that police took to identify the defendant is material to the outcome of the case. A misidentification defense relies on the quality of the identification procedure, so when that procedure is called into question,

152. Najibi, *supra* note 8.
153. Brady v. Maryland, 373 U.S. 83, 87 (1963).
154. *Kyles*, 514 U.S. at 420.
155. *See id.* at 447.
156. *Id.*
157. OPEN TECHNOLOGY INSTITUTE ET AL., CIVIL RIGHTS CONCERNS REGARDING LAW ENFORCEMENT USE OF FACE RECOGNITION TECHNOLOGY 5, n.26 (2021), https://newamericadotorg.s3.amazonaws.com/documents/FINAL_Civil_Rights_Statement_of_Concerns_LE_Use_of_FRT_June_2021.pdf [https://perma.cc/BM8U-X8GW].

there is a reasonable probability that it can change the outcome of a case. The crux of these arguments lies in the question of whether the facial recognition software was the witness' sole reason for identifying the defendant as the suspect.

4. The Probe Photo Used to Conduct the Search

The probing photo would qualify as Brady material for two reasons: (1) if the probing photo used in a facial recognition system is of poor quality, or (2) if the probe image has defining characteristics that undermine comparison to the defendant.[158] Both of these scenarios make this evidence material to the case and possibly exculpatory.

As explained above, a poorly lit, positioned, or pixilated image run through a facial recognition search comes with a higher possibility of inaccuracy.[159] Evidence of a poor probe image is material to the defendant's misidentification case because it could serve to support the argument that a faulty search was committed. The quality of the search is an important issue in a case in which the police rely solely on the facial recognition search to identify a suspect.

The second reason the probe image could be *Brady* material is because that photo could create doubt among members of the jury regarding whether the defendant is in fact the correct suspect. The touchstone of materiality is a "reasonable probability" of a different result, and the adjective is important. A "reasonable probability" of a different result is accordingly shown when the government's evidentiary suppression undermines confidence in the outcome of the trial.[160] If a photo is shown to the jury that would cast doubt on whether the defendant is the correct suspect, there is a strong possibility that the outcome of the trial may change. If the probe photo does not favor the defendant, that piece of evidence would also be exculpatory towards the defendant, thereby rendering it *Brady* material.

C. Facial Recognition Ensures Fair Treatment: It Is Not a Governmental Burden

Because facial recognition is so widely used by police departments in the U.S., some would argue that automatic disclosure and access to the details of its usage may impose too much of a burden on the government. However, given that facial recognition in federal criminal proceedings and investigations is ungoverned by any law, there are no better safeguards to ensure fair treatment under this technology. Until this area is regulated, the courts need to protect defendants' constitutional rights to a fair trial. Some may argue that because the evidence may only be exculpatory for criminal

158. ROGER RODRIGUEZ, FACIAL RECOGNITION: ART OR SCIENCE? 9, https://www.sheriffs.org/sites/default/files/Whitepaper%20Facial%20Recognition.pdf [https://perma.cc/XK97-TG62].

159. Amici Curiae Brief of ACLU et al., *supra* note 5, at 5.

160. *United States v. Bagley*, 473 U.S. 667, 678 (1985).

defendants of a specific race and/or gender, the need for disclosure to all defendants is not necessary. However, *Brady* material is assessed on factors within an individual case, and, thus, if the details of facial recognition are not relevant to a given defendant, then disclosure would not be required. This Note focuses on cases where the technology impacts the defendant negatively.

IV. CONCLUSION

In conclusion, use of facial recognition technology should be disclosed where the defendant could be exonerated given the nature of the facial recognition technology relied on by police. If Mr. Lynch was notified that the police solely relied on FACES to identify him during pre-trial discovery instead of eight days prior to his pretrial conference, he would have had a better opportunity to formulate his misidentification defense.

The purpose of the *Brady* rule is to ensure that defendants receive a fair trial and in order for a trial to be fair, they must have a chance to defend themselves based on any existing evidence that could aid their defense. If the prosecution withholds this evidence, a defendant will have no chance at a fair trial and could lose their liberty without ever receiving adequate due process. Due process is a constitutional right, and it should be treated with great importance. Until there are national standards set to improve the accuracy of facial recognition technology for all people, not just those that the technology does not negatively impact, defendants should have a right to access evidence regarding how that technology may have been the cause of police misidentification.