YOU CAN SEE MY FACE, WHY CAN'T I? FACIAL RECOGNITION AND *BRADY*

Rebecca Darin Goldberg*

TABLE OF CONTENTS

---

* J.D. Candidate 2021, Columbia Law School; B.A. 2015, Tufts University. The author would like to thank Professor Daniel Richman for his invaluable guidance and encouragement. The author would also like to thank the Honorable Jed S. Rakoff for his ongoing support, Saritha Komatireddy for her generous feedback, and the staff of the *Columbia Human Rights Law Review* for their editorial assistance. In addition, the author acknowledges the unwavering support of her parents, Marc and Donna, sister, Haley, and partner, Mike.

INTRODUCTION

On September 12, 2015, two undercover narcotics detectives driving around Jacksonville, Florida, were flagged down by a Black man who asked them, "[y]ou good?"[1] One of the detectives responded that he was looking for $50 worth of crack cocaine.[2] The man went inside a nearby residence, returned moments later, and exchanged the drugs for cash.[3] Taken by surprise when the man approached them, the detectives' typical surveillance equipment was not activated during the exchange.[4] Knowing that they would need to know the identity of the man in order to later arrest him, one of the detectives pretended to take a call on his cellphone so he could discreetly snap photographs.[5] Before the detectives drove away, the man said to them, "you see me around, my name is Midnight."[6]

The detectives sent the photographs to the Jacksonville Sheriff's Office Crime Analyst, who ran one photograph through a facial recognition system to see if it would match with any arrest photographs in the county.[7] The system provided several possible matches, but none of the results had greater than "one-star" confidence[8] of being correct.[9] The crime analyst sent only the first result, containing Willie Lynch's photograph, to the officers, along with Lynch's criminal history.[10] The officers accepted the crime analyst's suggestion and arrested Lynch.[11] But as Somil Trivedi, a senior staff attorney at the ACLU, put it, "anyone who's used Yelp can figure out

---

1. Benjamin Conarck, *How a Jacksonville Man Caught in the Drug War Exposed Details of Facial Recognition*, FLA. TIMES-UNION (May 26, 2017), https://www.jacksonville.com/news/metro/public-safety/2017-05-26/how-jacksonville-man-caught-drug-war-exposed-details-police [https://perma.cc/AQ92-WX3Y].
2. *Id.*
3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.*
7. Brief for ACLU et al. as Amici Curiae Supporting Petitioner at 3, Lynch v. State, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018) (No. SC 2019-0298).
8. Confidence levels are used in all facial recognition searches to establish how certain the algorithm is that the match generated is a correct match. *See infra* Section I.A; Jennifer Lynch, *Face Off: Law Enforcement Use of Facial Recognition Technology*, ELEC. FRONTIER FOUND. (Feb. 12, 2018), https://www.eff.org/wp/law-enforcement-use-face-recognition [https://perma.cc/X723-AQJT].
9. Brief for ACLU, *supra* note 7, at 3.
10. *Id.*
11. *Id.*; Conarck, *supra* note 1 (discussing the investigative techniques used).

that [one-star confidence is] not a high degree of confidence in your restaurant choice for lunch."[12]

At trial, the state's case was based on the detectives' testimony claiming they recognized the defendant as the man who had sold them drugs.[13] Lynch's defense was that they had the wrong guy.[14] Despite the Supreme Court's holding in *Brady v. Maryland*, mandating that a defendant have access to exculpatory information,[15] the state did not disclose to Lynch any of the other matches that the facial recognition system provided, nor did it inform him about the confidence levels of the matches.[16] The jury convicted Lynch, and the judge sentenced him to eight years.[17]

For Lynch and many other defendants who are involved in criminal cases in which facial recognition software is used, receiving exculpatory information under *Brady* could be the difference between a guilty verdict and an acquittal.[18] The use of facial recognition software has become a routine investigative tool for police agencies across the country, and is on track to become one of the most pervasive surveillance technologies relied on by law enforcement.[19] Despite its growing use, *Lynch v. State* appears to

---

12. Jack Karp, *Facial Recognition Software Sparks Transparency Battle*, LAW360 (Nov. 3, 2019), https://www.law360.com/articles/1215786/facial-recognition-software-sparks-transparency-battle [https://perma.cc/HD8B-RSMN].

13. Somil Trivedi & Nathan Freed Wessler, *Florida Is Using Facial Recognition to Convict People Without Giving Them a Chance to Challenge the Tech*, ACLU (Mar. 12, 2019), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/florida-using-facial-recognition-convict-people [https://perma.cc/8M45-METZ].

14. *Id.*

15. Brady v. Maryland, 373 U.S. 83, 87–88 (1963).

16. Trivedi & Wessler, *supra* note 13; Brief for the Petitioner, *supra* note 7, at 15 (discussing the prosecutor's disclosure to Lynch).

17. Conarck, *supra* note 1.

18. The Federal Bureau of Investigation (FBI) alone has performed more than 390,000 facial recognition searches in criminal cases. Trivedi & Wessler, *supra* note 13; U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-579T, FACE RECOGNITION TECHNOLOGY: DOJ AND FBI HAVE TAKEN SOME ACTIONS IN RESPONSE TO GAO RECOMMENDATIONS TO ENSURE PRIVACY & ACCURACY, BUT ADDITIONAL WORK REMAINS 6 (2019) [hereinafter GAO REPORT] (discussing the uses and implications of facial recognition).

19. Jon Schuppe, *How Facial Recognition Became a Routine Policing Tool in America*, NBC (May 11, 2019), https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251 [https://perma.cc/Q5H7-SJFA]; *Law Enforcement's Use of Facial Recognition Technology: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 115th Cong. 1 (2017) (statement of Kimberly J. Del Greco, Deputy Assistant Dir., Crim. Just. Info. Servs. Div., FBI); *see also* Lynch, *Face Off*, *supra* note 8 (discussing the uses of facial recognition technology); Ryan Mac et al., *Surveillance Nation*, BUZZFEED (Apr. 6, 2021), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition [https://perma.cc/YU9B-5LB5] (finding that law enforcement agencies across the United States have run thousands of

be the first case to raise *Brady* issues claiming that the use of the facial recognition software created exculpatory information.[20]

Part I of this Note provides a general overview of facial recognition software and the differences between facial recognition and other types of biometric data. Part II applies *Brady* to facial recognition software, detailing how defendants are not receiving potentially exculpatory information and discussing the due process implications of such inaction. Part III suggests that law enforcement agencies, courts, and Congress make changes to ensure the fair and effective[21] use of facial recognition.

I. THE BENEFITS AND RISKS OF FACIAL RECOGNITION SOFTWARE

This Part explores how facial recognition is currently used in criminal cases and how it is different from other forms of biometric data. This Part will focus on the FBI's facial recognition systems, since these are the most widely used.[22] Section I.A describes facial recognition and highlights the benefits and drawbacks of its application to criminal cases. Section I.B briefly examines the FBI's facial recognition system. Section I.C discusses challenges to facial recognition, including its accuracy and misuse. Section I.D addresses the fact that facial recognition is currently only publicly used as an investigative tool. Finally, Section I.E describes eyewitness identification, a central component of the use of facial recognition, and the implications of its fallibility.

A. What is Facial Recognition and How Does it Work?

Facial recognition has become a staple investigatory tool for law enforcement around the world.[23] While a few American states and cities

---

Clearview AI facial recognition searches, "often without the knowledge of the public or even their own departments").

20. Trivedi & Wessler, *supra* note 13.

21. While this Note focuses on the misuse and inaccuracies of facial recognition, the technology could potentially be harnessed for effective use. With proper measures, discussed in more detail in Part III, facial recognition may be safely used to both correctly identify suspects and exculpate wrongfully accused criminal defendants.

22. Neema Singh Guliani, *The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database*, ACLU (June 7, 2019), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through [https://perma.cc/FM8G-SBU2].

23. Sinitia Radu, *The Technology That's Turning Heads*, U.S. NEWS (July 26, 2019), https://www.usnews.com/news/best-countries/articles/2019-07-26/growing-number-of-countries-employing-facial-recognition-technology [https://perma.cc/CQ77-PG5Z].

have banned its use,[24] many of the nation's most influential police departments, including those in New York City and Chicago, use facial recognition.[25] The technology is so widespread that, in 2010, the FBI began replacing its fingerprinting system with Next Generation Identification (NGI) facial recognition technology.[26]

In general, facial recognition software works by creating a map of facial features from a probe photograph and comparing that information to a database of stored images.[27] Most Americans are now part of these databases[28] as photographs in the databases are sourced from driver's licenses, government identification records, mugshots, and social media accounts. The specific source(s) depends on the law enforcement agency.[29]

Compared to other forms of biometric data, facial recognition programs are unique in their matching process.[30] Most facial recognition

---

24. California, New Hampshire, and Oregon currently ban the use of facial recognition technology in police body cameras. Oakland and San Francisco ban the use of facial recognition by city agencies, including police departments. In Massachusetts, Brookline and Somerville have both banned facial recognition. New York and New Jersey are considering bans on facial recognition. Max Read, *Why We Should Ban Facial Recognition Technology*, N.Y. MAG. (Jan. 30, 2020), https://nymag.com/intelligencer/2020/01/why-we-should-ban-facial-recognition-technology.html [https://perma.cc/7RH4-7ESA]; Jason Tashea, *As Facial Recognition Software Becomes More Ubiquitous, Some Governments Slam on the Brakes,* A.B.A. J. (Sept. 24, 2019), http://www.abajournal.com/web/article/facial-recog-bans [https://perma.cc/7HBU-6548] (discussing various bans on facial recognition technology).

25. *Ban Facial Recognition Map*, FIGHT FOR THE FUTURE, https://www.banfacialrecognition.com/map/ [https://perma.cc/M7AP-KTNE].

26. NGI includes both fingerprint and facial recognition capabilities. *S*ee GAO REPORT, *supra* note 18. In 2017, the FBI used the facial recognition component of NGI to assist in the identification and arrest of an individual on the FBI Ten Most Wanted Fugitive list. *Id.* at 1.

27. Kevin Bonsor & Ryan Johnson, *How Facial Recognition Systems Work*, HOW STUFF WORKS (July 26, 2019), https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition1.htm [https://perma.cc/GM3S-2N9H].

28. *Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. 5 (2019) (statement of Clare Garvie, Senior Assoc., Ctr. on Priv. and Tech. at Geo. L.), https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-GarvieC-20190522.pdf [https://perma.cc/7Y2H-NJ77] [hereinafter Statement of Clare Garvie].

29. Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will it Take Us?*, A.B.A. CRIM. JUST. MAG. (Spring 2019), https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/ [https://perma.cc/F95H-B4PE].

30. *Compare DNA Evidence Basics: Possible Results from Testing*, NAT'L INST. OF JUST. (Aug. 8, 2012), https://nij.ojp.gov/topics/articles/dna-evidence-basics-possible-results-

systems calculate a probability match score, or a confidence score, between an unknown person and known persons in the database.[31] They offer several possible matches ranked in order of likelihood and provide confidence levels to accompany each match.[32] DNA and fingerprint comparisons, on the other hand, indicate whether the DNA profile or fingerprint ridges, respectively, matches the DNA profile or fingerprint at the crime scene.[33] If the sample is contaminated or does not have enough of the biometric data, either insufficient DNA or a partial latent fingerprint, the result is inconclusive.[34] Facial recognition is different; even if the matches include the correct suspect, the analyst conducting the search and selecting the match to forward to investigators may choose the wrong individual.[35] The correct match may not even be in the list of results identified by the software, but the analyst reviewing the results may find a match anyway, thereby implicating an innocent person (a false positive).[36]

---

testing [https://perma.cc/MTB8-24P7] (discussing DNA analysis), *with* GAO REPORT, *supra* note 18 (discussing facial recognition analysis).

31. Lynch, *supra* note 8, at 7.

32. *Id.*

33. William Harris, *How DNA Evidence Works*, HOW STUFF WORKS (Jan. 18, 2001), https://science.howstuffworks.com/life/genetic/dna-evidence4.htm [https://perma.cc/J5W2-ZXET] (discussing DNA analysis).

34. *Id.* Familial DNA testing, in which law enforcement looks for similar DNA profiles to find relatives of the suspect, uses either custom-designed software to produce a list of ranked candidates or genealogy sites such as GEDMatch to list known relatives. EMILY NIEDZWIECKI ET AL., NAT'L CRIM. JUST. REFERENCE SERV., OFF. OF JUST. PROGRAMS, UNDERSTANDING FAMILIAL DNA SEARCHING: COMING TO A CONSENSUS ON TERMINOLOGY 1–4 (2017), available at https://www.ncjrs.gov/pdffiles1/nij/grants/251080.pdf [https://perma.cc/CA3Z-NZL5]; DEP'T OF JUST., INTERIM POLICY, FORENSIC GENETIC GENEALOGICAL DNA ANALYSIS AND SEARCHING (2019), available at https://www.justice.gov/olp/page/file/1204386/download [https://perma.cc/Y9PJ-FDCR]. For an in-depth discussion of the difficulties with partial prints, see OFF. OF THE INSPECTOR GEN., DEP'T OF JUST., A REVIEW OF THE FBI'S HANDLING OF THE BRANDON MAYFIELD CASE (2006), available at https://oig.justice.gov/special/s0601/final.pdf [https://perma.cc/7QWV-AQK6].

35. Kaitlin Jackson, *Challenging Facial Recognition in Court*, 43 CHAMPION 14, 16 (2019).

36. INTEGRATED JUST. INFO. SYS. INST., LAW ENFORCEMENT FACIAL RECOGNITION USE CASE CATALOG 2 (2019) [hereinafter IJIS INST.], https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/Law_Enforcement_Facial_Recognition_Use_Case_Catalog.pdf [https://perma.cc/3LM8-RUL9]. False positives "are the erroneous association of samples of two persons; they occur when the digitized faces of two people are similar." PATRICK GROTHER ET AL., DEP'T OF COM., NISTIR 8280, FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 1–3 (2019), available at https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf [https://perma.cc/4LL3-TYYF].

B. The FBI's Facial Recognition System

The FBI has access to hundreds of millions of photographs[37] and has said that facial recognition is critical to its mission.[38] The FBI has two programs that use facial recognition: the Next Generation Identification System Interstate Photo System (NGI-IPS), for external agencies, and the Facial Analysis, Comparison, and Evaluation (FACE) Services, which is internal to the FBI.[39] As of April 2019, the collective databases searchable by FACE contained 641 million photographs.[40] When FBI agents request a search, biometric image specialists within the FBI FACE Services unit review any matches received from external partners before releasing results.[41] Unlike NGI-IPS, which returns between two and fifty results depending on the user's specification, when a search is conducted using FACE, a specialist completes a review, and no more than two photos are returned as a lead to the requesting FBI agent.[42] The number of results is relevant to defendants who are seeking this information as part of *Brady* disclosure because additional results can help defendants make a case that an alternative suspect may have been the perpetrator.[43]

C. Challenges with Facial Recognition Accuracy and Misuse

Facial recognition's use is expanding in part due to the increased availability of photos.[44] It is becoming increasingly likely that crimes will be

---

37. GAO REPORT, *supra* note 18, at 6.

38. Stephen Rex Brown, *A Florida Drug Case Could Set Precedent for Facial Recognition in Policing*, GOV'T TECH. (Mar. 21, 2018), https://www.govtech.com/public-safety/A-Florida-Drug-Case-Could-Set-Precedent-for-Facial-Recognition-in-Policing.html [https://perma.cc/KBQ4-8EW3].

39. Dakin Andonne, *Police Used Facial Recognition to Identify the Capital Gazette Shooter. Here's How It Works*, CNN (June 29, 2018), https://www.cnn.com/2018/06/29/us/facial-recognition-technology-law-enforcement/index.html [https://perma.cc/L9Z8-4ZM6].

40. GAO REPORT, *supra* note 18, at 6.

41. *Id.*

42. *Id.* at 3, 6.

43. *See, e.g.*, Boyette v. Lefevre, 246 F.3d 76, 91 (2d Cir. 2001) (finding that documents were *Brady* material because they could have helped the defense suggest an alternative perpetrator).

44. Joseph Clarke Celentino, *Face-to-Face with Facial Recognition Evidence: Admissibility Under the Post-Crawford Confrontation Clause*, 114 MICH. L. REV. 1317, 1324 (2016); Cade Metz, *Facial Recognition Tech Is Growing Stronger, Thanks to Your Face*, N.Y. TIMES (July 13, 2019), https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html (on file with the *Columbia Human Rights Law Review*) (discussing the increasing use of facial recognition).

caught on camera,[45] which will in turn contribute to law enforcement's increased use of facial recognition software. There are reasons to be concerned about this increased reliance, however, due to issues with the accuracy of facial recognition.[46]

The accuracy of facial recognition systems, measured by whether the software correctly identifies the person in the probe photograph, can vary based on a number of factors, including camera quality, light, distance, database size, algorithm, and the target's race and gender.[47] Generally, advanced systems can achieve false positive error rates below 10%.[48] In 2016, the FBI reported that their systems successfully included the correct candidate in a list of fifty potential matches only 86% of the time.[49] In other words, one out of every seven searches returned a list of fifty innocent candidates (and failed to identify a correct match).[50]

False positives are especially problematic in criminal cases because they provide law enforcement with an incorrect identity, which can lead investigators to pursue an innocent person. Furthermore, facial recognition software varies across law enforcement agencies,[51] and many agencies have

---

45. Celentino, *supra* note 44 ("In short, the chances that a crime will either be caught on film or that a perpetrator's facial data will be on file can be expected to increase with time.").

46. 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 (on file with the *Columbia Human Rights Law Review*).

47. *See id.*; Jake Laperruque, *Unmasking the Realities of Facial Recognition*, PROJECT ON GOV'T OVERSIGHT (Dec. 5, 2018), https://www.pogo.org/analysis/2018/12/unmasking-the-realities-of-facial-recognition/ [https://perma.cc/S2RK-8L46] (discussing factors affecting facial recognition accuracy).

48. This means 90% of the time the result is accurate. The false positive rate is how often the technology incorrectly generates a match to a known person in the database; the detection rate is how often the technology generates a match when the person is known to be in the database. GAO REPORT, *supra* note 18, at 14. False positives "are the erroneous association of samples of two persons; they occur when the digitized faces of two people are similar." False negatives, on the other hand, "are the failure to associate one person in two images; they occur when the similarity between two photos is low." GROTHER ET AL., *supra* note 36, at 2; *see also* GAO REPORT, *supra* note 18 (discussing the importance of knowing the false positive rate).

49. GAO REPORT, *supra* note 18, at 14.

50. Sam Levin, *Half of U.S. Adults Are Recorded in Police Facial Recognition Databases, Study Says*, THE GUARDIAN (Oct. 18, 2016), https://www.theguardian.com/world/2016/oct/18/police-facial-recognition-database-surveillance-profiling [https://perma.cc/SZ5S-SKEN]. The FBI had not, however, assessed how often NGI-IPS face recognition searches erroneously matched a person to the database (the false positive rate). GAO REPORT, *supra* note 18, at 14.

51. GARVIE ET AL., GEO. L. CTR. ON PRIV. & TECH., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 2 (2016), available at

lower standards of accuracy than the FBI or do not conduct accuracy tests at all.[52] In 2019, the FBI announced its plan to use a new vendor that claims an accuracy rate of over 99%, [53] but due to incomplete reporting on accuracy, there is reason to doubt this figure.[54]

Though there are almost eighteen thousand local police agencies in the United States,[55] there exist no uniform standards or regulations for facial recognition software.[56] Therefore, police departments across the U.S. differ in their uses of facial recognition software with varied levels of accuracy, some of which have even been described as "fringe techniques."[57]

---

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/VA5B-MQKV].

52. *Id.* at 46–52.

53. *The Use of Facial Recognition Technology by Government Entities and the Need for Oversight of Government Use of This Technology Upon Civilians: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. 4 (2019) (statement of Kimberly J. Del Greco, Crim. Just. Info. Servs. Div., FBI) [hereinafter Statement of Kimberly J. Del Greco, 2019].

54. To address the concerns regarding the accuracy of the FBI's facial recognition system, the U.S. Government Accountability Office (GAO) made three recommendations, which, as of June 2019, the FBI has failed to address: conduct accuracy tests on different result sizes; assess overall accuracy of the software; and evaluate the accuracy when outside agencies use the software. GAO REPORT, *supra* note 18. Current accuracy tests have been performed on larger-than-typical result sizes, in unrealistic settings and environments, and with unknown detection rates. *Id.* at 14. Compounding this issue, the FBI did not conduct accuracy tests on its operational database. *Id.* at 16. This assessment was done on a database 25 times smaller than the current FBI facial recognition database, and, generally, errors increase with database size. GARVIE ET AL., *supra* note 51, at 67. Thus, the FBI has allowed external partners to conduct facial recognition searches without knowing how accurate they are. *Id.* at 66–67. While the FBI is working to address the shortcomings of its programs, DOJ officials have said that the FBI has no authority to set or enforce accuracy standards for facial recognition run by other law enforcement agencies. *Id.* at 17–18. It is unknown how many criminal defendants have been implicated in searches with questionable levels of accuracy, but given the number of searches per month, it is likely there are at least thousands. Trivedi & Wessler, *supra* note 13; GARVIE ET AL., *supra* note 51, at 2–3 (discussing the number of law enforcement searches using facial recognition).

55. Jon Greenberg, *How Many Police Departments Are in the United States?*, POLITIFACT (July 10, 2016), https://www.politifact.com/punditfact/statements/2016/jul/10/charles-ramsey/how-many-police-departments-are-us/ [https://perma.cc/3YP5-QP3T].

56. GARVIE ET AL., *supra* note 51, at 1.

57. Jim Trainum, *Facial Recognition Surveillance Doesn't Necessarily Make You Safer*, PROJECT ON GOV'T OVERSIGHT (July 22, 2019), https://www.pogo.org/analysis/2019/07/facial-recognition-surveillance-doesnt-necessarily-make-you-safer/ [https://perma.cc/8YAQ-VE3J]. In 2017, the NYPD used a "fringe technique" by submitting a Google image search photograph of the actor Woody Harrelson into the NYPD's facial recognition system, when the footage containing the suspect's image had

The same is not true for DNA evidence, which, when used through the National DNA Index System (NDIS) or the Combined DNA Index System (CODIS), has strict and standardized requirements.[58]

There are neither accuracy requirements for facial recognition software nor standards for what law enforcement can submit as probe photographs.[59] Because probe photographs in criminal cases often come from surveillance footage, most probe photographs are imperfect: they are often low resolution and not front-facing.[60] In order to overcome these imperfections, some law enforcement agencies allow officers to substantially edit the photographs by replacing facial features on the probe photograph with those from stock photographs or by digitally approximating the other side of the face.[61] The more editing that is done to the probe photograph, however, the less reliable the results.[62]

Moreover, facial recognition technology is particularly inaccurate when identifying women, people of color, and young people.[63] According to

---

such poor quality that it yielded no results. Using the photograph of Woody Harrelson, the facial recognition system listed several results, and the NYPD made an arrest. The outcome of the case has not been revealed. Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. L. CTR. ON PRIVACY & TECH. (May 16, 2019), https://www.flawedfacedata.com/ [https://perma.cc/CQW3-E5QM].

58. *Frequently Asked Questions on CODIS and NDIS*, FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet [https://perma.cc/R8CJ-SR39]; *CODIS—NDIS Statistics*, FBI (Sept. 2019), https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics [https://perma.cc/4MLT-QAH9]. *But see* Jason Kreag, *Articles Going Local: The Fragmentation of Genetic Surveillance*, 95 B.U. L. REV. 1491, 1494 (2015) (discussing how some local law enforcement agencies are creating their own DNA databases).

59. Garvie, *supra* note 57.

60. Jackson, *supra* note 35, at 15; GARVIE ET AL., *supra* note 51, at 47 (discussing the wide range of settings in which probe photos are taken).

61. Jackson, *supra* note 35, at 15.

62. Garvie, *supra* note 57. Furthermore, at least half a dozen police departments permit, and some even encourage, the use of forensic sketches in facial recognition searches. *Id.*

63. Trainum, *supra* note 57; Lohr, *supra* note 46 (discussing a study that measures how the technology works on people of different races and genders); Tim Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, WIRED (July 22, 2019), https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/ [https://perma.cc/2NQZ-C54A] (discussing a finding that a particular company's facial recognition software falsely matched black women's faces ten times more likely than white women's faces); Brendan F. Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 IEEE TRANSACTIONS ON INFO. FORENSICS & SEC. 1789, 1791, 1789–1801 (2012) (discussing study results showing that facial recognition algorithms consistently have lower matching accuracies with women, people of color, and young people than men, white people, and older people); Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender*

a study by the National Institute of Standards and Technology (NIST), the majority of facial recognition algorithms exhibit demographic differentials.[64] These inaccuracies increase the probability that people of color will improperly become investigative targets.[65] Despite the inaccuracies and inconsistencies in the way facial recognition is used, facial recognition continues to be heavily relied on by law enforcement.[66]

D. Facial Recognition as an Investigative Tool

Currently, facial recognition is principally used as an investigative technique to identify suspects who, thereafter, are identified by eyewitnesses or matched by a testifying witness to a surveillance photograph.[67] The software is purportedly not used on its own to establish probable cause for an arrest.[68] But research shows that in reality, many law

---

Classification, 81 PROC. OF MACHINE LEARNING RES. 1 (2018) (discussing an approach to evaluate bias in facial analysis algorithms). In one study, Amazon's facial recognition technology, Rekognition, incorrectly matched 28 members of Congress, mistakenly identifying them as other people who have been arrested. The false matches were disproportionately people of color. Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (July 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [https://perma.cc/7HQB-DJE6].

64. *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NAT'L INST. OF STANDARDS & TECH. (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software [https://perma.cc/5RVR-YGJK].

65. Trainum, *supra* note 57.

66. Facial recognition can help deter crime due to the increased presence of surveillance and lead to arrests once a suspect has been identified. Lynch, *Face Off*, *supra* note 8; Bernard Marr, *Facial Recognition Technology: Here Are the Important Pros and Cons*, FORBES (Aug. 19, 2019), https://www.forbes.com/sites/bernardmarr/2019/08/19/facial-recognition-technology-here-are-the-important-pros-and-cons/#2c3775a614d1 [https://perma.cc/QUQ9-5B46] (discussing some of the benefits of using facial recognition).

67. Hamann & Smith, *supra* note 29; Julie Bosman & Serge F. Kovaleski, *Facial Recognition: Dawn of Dystopia, or Just the New Fingerprint?*, N.Y. TIMES (May 18, 2019), https://www.nytimes.com/2019/05/18/us/facial-recognition-police.html (on file with the *Columbia Human Rights Law Review*) (discussing how facial recognition is used in criminal investigations).

68. The Jacksonville Sheriff's Office, in response to an inquiry about *Lynch*, stated that detectives only use FACES in conjunction with other investigatory tools. Aaron Mak, *Facing Facts*, SLATE (Jan 25, 2019), https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html [https://perma.cc/BK3X-QFB5]; Hamann & Smith, *supra* note 29 (discussing how facial recognition is used in criminal investigations). Former NYPD Commissioner James O'Neill recently wrote that "no one can be arrested on the basis of the computer match alone." James O'Neill, *How Facial Recognition Makes You Safer*, N.Y. TIMES (June 9, 2019), https://www.nytimes.com/

enforcement agencies have relied almost exclusively on facial recognition systems to make an arrest.[69] Further, even if the results produced by the technology are used as a lead and confirmed by an eyewitness, eyewitness identifications are notoriously unreliable.[70]

E. Issues with Eyewitness Identification in Criminal Cases

The disclosure of facial recognition results is particularly important due to established fallibility regarding eyewitness identification and human memory.[71] While eyewitness identification is among the most common types of evidence admitted into courtrooms, it is also one of the most problematic due to the rate of misidentification.[72] In fact, a recent study by the Innocence Project found that 75% of wrongful convictions in the U.S. have involved eyewitness misidentification.[73] Given the problems with eyewitness identification and the fact that eyewitness misidentification is

---

2019/06/09/opinion/facial-recognition-police-new-york-city.html (on file with the *Columbia Human Rights Law Review*). This practice was confirmed by court documents surveyed by the New York Times, in which facial recognition was not listed in initial warrants or affidavits. Instead, detectives cited "investigative means" or "attempt to identify. 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 (on file with the *Columbia Human Rights Law Review*).

69. Statement of Clare Garvie, *supra* note 28, at 16. For example, in April of 2019, a police officer investigating a theft in Tallahassee obtained an image from store surveillance and received a likely match from the facial recognition system. Valentino-DeVries, *supra* note 68. The investigator reviewed the store surveillance video, positively identified the suspect, and stated there was probable cause for an arrest on that basis. Tallahassee Police Department Field Case Supplement (2019), https://www.documentcloud.org/documents/6586364-Targettheft-Redacted.html [https://perma.cc/3MJV-7J6C]; Valentino-DeVries, *supra* note 68 (discussing instances where facial recognition was the primary basis for an arrest).

70. *See generally* Gary L. Wells & Elizabeth A. Olson, *Eyewitness Testimony*, 54 ANNU. REV. PSYCHOL. 277 (2003) (outlining the dangers of eyewitness testimony). One study found that passport-system employees, who are trained in identification, have trouble identifying the correct person on a list of similar-looking facial recognition results half the time. David White et al., *Error Rates in Users of Automatic Face Recognition Software*, 10 PLOS ONE 1, 1 (2015).

71. *See generally* INNOCENCE PROJECT, REEVALUATING LINEUPS: WHY WITNESSES MAKE MISTAKES AND HOW TO REDUCE THE CHANCE OF A MISIDENTIFICATION (2009), https://www.innocenceproject.org/wp-content/uploads/2016/05/eyewitness_id_report-5.pdf [https://perma.cc/9D4K-6ZEK] (analyzing the fallibility of eyewitness testimony). *See also* United States v. Nolan, No. 16-3423-PR, 2020 WL 1870140, at *5–7 (2d Cir. Apr. 15, 2020) (discussing the inaccuracies of eyewitness identification).

72. INNOCENCE PROJECT, *supra* note 71.

73. *Id.*

associated with more wrongful convictions than any other cause,[74] disclosure of the process used to identify a defendant is all the more important. Courts have recognized the importance of this type of evidence and found that "[i]dentification testimony may be outcome determinative" and is therefore required to be disclosed to defense counsel.[75]

The inclusion of a suspect selected by facial recognition in an identification procedure may increase the chance of eyewitness misidentification because eyewitnesses are likely to positively identify look-alikes, regardless of whether the look-alikes are actually the perpetrator.[76] Moreover, facial recognition programs are *specifically designed* to produce results that look like the perpetrator.[77] Misidentification occurs less frequently in cases in which the eyewitness knows the defendant well,[78] yet most cases using facial recognition involve a police officer serving as an in-court witness testifying to having seen the event or having compared the match photograph to the suspect.[79] The issue

---

74. JUST. PROJECT, EYEWITNESS IDENTIFICATION: A POLICY REVIEW 2 (2007), https://web.williams.edu/Psychology/Faculty/Kassin/files/Justice%20Project%20-%20on%20ET.pdf [https://perma.cc/72A6-RYN5]; Brian Gregory, Brady *Is the Problem: Wrongful Convictions and the Case for "Open File" Criminal Discovery,* 46 U.S.F.L. REV. 819, 839 (2012) (discussing false eyewitness identification).

75. Williams v. State, 364 Md. 160, 174 (2001); *see also* Kyles v. Whitley, 514 U.S. 419, 441–44 (1995) (finding a *Brady* violation when prosecution failed to disclose eyewitness descriptions of perpetrator that were not consistent with defendant); White v. Helling, 194 F.3d 937, 943 (8th Cir. 1999) (finding a *Brady* violation when prosecutor failed to disclose that witness had initially identified another person as performing key actions during the robbery); McDowell v. Dixon, 858 F.2d 945, 949 (4th Cir. 1988) (finding a *Brady* violation when prosecution failed to disclose that initial witness statement had indicated perpetrator was a different race than defendant); Curry v. United States, 658 A.2d 193, 195, 197 (D.C. 1995) (noting that the government conceded error when it failed to disclose until two days prior to trial statements of eyewitness whose description of the perpetrator was inconsistent with defendant).

76. Jackson, *supra* note 35, at 17.

77. *Id.* at 17.

78. *See* Haliym v. Mitchell, 492 F.3d 680, 706 (6th Cir. 2007) ("Witnesses are very likely to recognize under any circumstance the people in their lives with whom they are most familiar, and any prior acquaintance with another person substantially increases the likelihood of an accurate identification.").

79. *See* Bosman & Kovaleski, *supra* note 67 (considering the case of Robert Kusma, a suspect in the sexual assault of a 15-year-old girl). His name was unknown at the time of the crime. The victim provided the police with a photograph of the suspect. Police ran the suspect's photograph in their facial recognition software several times, but there was no match. In December 2018, a match was made to Kusma's new driver's license ID. The investigating officer compared the match to the picture from victim's phone, concluded it was the defendant, and arrested Kusma. In cases involving facial recognition, the additional step to confirm the suspect's identity requires eyewitness identification. *Id.*

is plain: investigations that use facial recognition to identify the suspect rely both on technology with unreliable levels of accuracy and on humans with unreliable capabilities of identification.[80]

Not only are facial recognition and human identification fallible on their own, but also errors in facial recognition can be compounded through suggestive identification procedures.[81] Suggestive procedures can occur when law enforcement signals to witnesses that facial recognition has been used.[82] When law enforcement tells eyewitnesses that facial recognition was used, eyewitnesses may have a false belief that the perpetrator must be present in the photographs presented,[83] thereby increasing the chances that the wrong individual is selected.

Suggestiveness of facial recognition is a serious concern as it can increase the likelihood of misidentification.[84] In the context of biometric data, however, suggestiveness is a problem that is unique to facial recognition because neither DNA nor fingerprint analysis involves eyewitness identification procedures. Despite this difference, the results of DNA and fingerprint analysis are consistently turned over to defense, while facial recognition results are not.[85] When facial recognition is used, the analyst who conducts the search knows what the suspect looks like.[86] Once the facial recognition system releases results, the analyst conducts a visual analysis to identify a match and determine the identity of the suspect.[87] This identification procedure is ripe for misidentification because while the software releases several possible matches, the analyst conducting the search makes the final identification.[88]

---

80. *See generally* Jed S. Rakoff & Elizabeth F. Loftus, *The Intractability of Inaccurate Eyewitness Identification*, 147 DAEDALUS: J. AMER. ACAD. ARTS & SCI. 90 (2018) (discussing the unreliability of eyewitness testimony).

81. Jackson, *supra* note 35, at 22.

82. *Id.*; Lane Brown, *There Will Be No Turning Back on Facial Recognition*, N.Y. MAG. (Nov. 12, 2019), http://nymag.com/intelligencer/2019/11/the-future-of-facial-recognition-in-america.html [https://perma.cc/KB5Y-AH63].

83. Jackson, *supra* note 35, at 22.

84. *Id.*

85. Brady *Disclosure Requirements,* INT'L ASS'N. OF CHIEFS OF POLICE (IACP) NAT'L L. ENF'T POL'Y CTR. (2008), https://www.theiacp.org/sites/default/files/all/b/BradyPaper.pdf [https://perma.cc/2WMY-HXGK]; Ira Mickenberg, *A Practical Guide to* Brady *Motions: Getting What You Want, Getting what You Need,* NEW FELONY DEF. PROGRAM (2008), http://www.ncids.org/Defender%20Training/2008%20New%20Felony%20Defender%20Training/BradyHandout.pdf [https://perma.cc/GHG3-Z328] (discussing discovery practices for biometric data).

86. Jackson, *supra* note 35, at 22.

87. *Id.*

88. *Id.*

Despite the fact that facial recognition increases the risk of misidentification,[89] information regarding facial recognition identification procedures is not disclosed to the defense.[90] The Supreme Court has said that "the vagaries of eyewitness identification are well-known; the annals of criminal law are rife with instances of mistaken identification."[91] In order to address the concerns of an "irreparable misidentification",[92] facial recognition identification results and confidence scores must be disclosed under *Brady.*

The next Part of this Note will apply *Brady* to facial recognition and will argue that information generated by facial recognition searches should qualify as *Brady* material and therefore be provided to defendants.

II. *BRADY* APPLIED TO FACIAL RECOGNITION

This Part imposes the *Brady* framework on the facial recognition context, detailing the justified concern that defendants are not receiving potentially exculpatory information with regard to facial recognition results. Section II.A discusses the scope of *Brady*. Section II.B explores the *Brady* concerns that surfaced in *Lynch v. State*. Section II.C reviews the *Brady* materiality standard and argues that facial recognition results and confidence scores are material. Section II.C also addresses concerns regarding *Brady*'s application to facial recognition when the technology is used only as an investigative tool.

A. Scope of the *Brady* Doctrine

In 1963, the Supreme Court announced, in *Brady v. Maryland*, one of the most significant rules for criminal defendants: prosecutors must disclose "exculpatory" evidence.[93] The Court held that "the suppression by the prosecution of evidence favorable to an accused upon request violates

---

89. *Id.* at 17.

90. *See infra* Section II.C.1.

91. United States v. Wade, 388 U.S. 218, 228 (1967).

92. Summitt v. Bordenkircher, 608 F.2d 247, 250–51 (6th Cir. 1979) ("The basis of the due process right against suggestive identification procedures is significantly different. It is, first of all, apparent that the primary evil to be avoided is a very substantial likelihood of irreparable misidentification." (citations omitted)) *aff'd sub nom* Watkins v. Sowders, 449 U.S. 341 (1981).

93. Brady v. Maryland, 373 U.S. 83, 87 (1963). John Brady and a companion, Boblit, were convicted of murder in the first degree and were sentenced to death. While Brady admitted to participating in the crime, he maintained that Boblit had killed the victim. Only after Brady was sentenced did he learn that the state withheld a statement in which Boblit admitted to committing the homicide. *Id.*

due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution."[94] The Court reasoned that suppression of such exculpatory information was a violation of the Due Process Clause of the Fourteenth Amendment.[95]

Despite the seemingly expansive rule, *Brady* is limited by the element of materiality. *Brady* demands the disclosure only of evidence that is "material" to the defendant's case,[96] but since the *Brady* Court did not provide a standard of "materiality," courts have interpreted this obligation

---

94. *Id.*

95. *Id.* at 86. Writing for the majority, Justice Douglas explained the significance of fairness for the accused: "[s]ociety wins not only when the guilty are convicted but when criminal trials are fair; our system of the administration of justice suffers when any accused is treated unfairly." *Id.* at 87; *see also* Miriam H. Baer, *Timing Brady*, 115 COLUM. L. REV. 1, 4 (2015) (discussing the fairness implications of *Brady*'s disclosure requirements). Subsequent cases expanded upon *Brady* to create additional protections for defendants. In *Giglio v. United States*, the Supreme Court clarified that all impeachment evidence, even if not a prior statement by a witness, falls within the *Brady* rule. *Giglio v. United States*, 405 U.S. 150 (1972). Furthermore, in *United States v. Bagley*, the Court abandoned the distinction between exculpatory and impeachment evidence. 473 U.S. 667, 676 (1985). Such evidence is "evidence favorable to an accused, so that, if disclosed and used effectively, it may make the difference between conviction and acquittal." *Id.* (internal citations omitted). Additionally, in *Kyles v. Whitley*, the Court held that the prosecutor has a duty to learn of, and disclose, any favorable evidence known to "others acting on the government's behalf in the case, including the police." 514 U.S. 419, 437 (1995). The prosecution has a duty not only to disclose evidence that is known to them and that is favorable to the defense and material to guilt or punishment. Turner v. United States, 137 S. Ct. 1885, 1888 (2017) ("In *Brady v. Maryland*, this Court held that the government violates the Constitution's Due Process Clause 'if it withholds evidence that is favorable to the defense and material to the defendant's guilt or punishment.'" (internal citations omitted)). The prosecution has an additional duty to learn of and disclose any such information known by law enforcement. Note, *The Prosecutor's Duty to Disclose to Defendants Pleading Guilty*, 99 HARV. L. REV. 1004, 1004 (1986); IACP NAT'L L. ENF'T POL'Y CTR., *supra* note 85 (discussing the duty to disclose exculpatory evidence). Any evidence that could negate a defendant's guilt, reduce a defendant's potential sentence, or affect the credibility of a witness is "*Brady* material." *Brady Rule*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/brady_rule [https://perma.cc/49R9-RGZA]. If a *Brady* violation is established post-trial, the conviction is reversed, and the defendant is granted a new trial. Barry Scheck & Nancy Gertner, *Combatting* Brady *Violations with an 'Ethical Rule' Order for the Disclosure of Favorable Evidence*, NAT'L ASS'N OF CRIM. DEF. LAWS. (May 2013), https://www.nacdl.org/Article/May2013-CombattingBradyViolationsWithA [https://perma.cc/4AUD-WLUG]; Cynthia E. Jones, *Here Comes the Judge: A Model for Judicial Oversight and Regulation of the* Brady *Disclosure Duty*, 46 HOFSTRA L. REV. 87, 89 (2017) (discussing remedies for *Brady* violations, including the power of courts to impose sanctions for *Brady* misconduct). Pre-trial violations are addressed by ordering disclosure. *Id*. at 91.

96. *Brady*, 373 U.S. at 87.

differently.[97] While many courts originally concluded that *Brady* requires the disclosure of *all* evidence favorable to the defendant, the Supreme Court has more recently made it clear that *Brady* requires only the disclosure of material exculpatory evidence.[98]

B. Facial Recognition Disclosure Concerns in *Lynch v. State*

Defendants have reason to seek information about the number of matches provided by a facial recognition search because if more than one result is provided, the defendant has a stronger case for mistaken identity. In *Lynch v. State*, although FACES, the facial recognition program, returned several possible matches to the cellphone photograph, the prosecution never disclosed this information.[99] The probe photograph taken of the suspect was blurry and captured from a side angle, and none of the search results expressed more than "one-star" confidence—information that would have strongly called the identification into question.[100] Notwithstanding the possibility of alternative suspects, the crime analyst sent only Lynch's name to the requesting officers.[101]

The Florida First District Court of Appeals rejected Lynch's *Brady* argument because the court found that Lynch did not show "a reasonable probability that the result of the trial would have been different if the suppressed documents had been disclosed to the defense."[102] The court reasoned that because Lynch could not show that the other facial recognition matches resembled him, he was unable to argue that they would have supported his contention that someone in one of the other results was the culprit.[103] The issue with this reasoning, however, is that the photographs were in the possession of law enforcement. When Lynch learned that facial recognition was used, he requested that the state disclose the photographs of the other potential matches.[104] The state

---

97. *Compare* United States v. Safavian, 233 F.R.D. 12, 16 (D.D.C. 2005) (requiring prosecutors to disclose all evidence favorable to defense in advance of trial), *and* United States v. Sudikoff, 36 F. Supp. 2d 1196, 1199 (C.D. Cal. 1999) (same), *with* United States v. Padilla, No. CR 09-3598 JB, 2010 WL 4337819, at *5 (D.N.M. Sept. 3, 2010) (criticizing standard in *Sudikoff* because it "would effectively require the government to produce all information rather than conduct a materiality review").

98. United States v. Ruiz, 536 U.S. 622, 628 (2002).

99. Brief for ACLU, *supra* note 7, at 1.

100. *Id.* at 2, 14.

101. *Id.* at 3.

102. Lynch v. State, 260 So. 3d 1166, 1170 (Fla. Dist. Ct. App. 2018) (citing Strickler v. Greene, 527 U.S. 263, 289 (1999)).

103. *Id.*

104. Motion for Rehearing and Written Opinion at 2, Lynch v. State, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018) (No. 1D16-3290).

refused, and Lynch was never able to view the other matches.[105] In rejecting Lynch's *Brady* argument, the court essentially "reward[ed] the state for its discovery violation."[106] On appeal, the Florida Supreme Court declined to hear the case for lack of jurisdiction.[107] *Lynch*, however, did not settle the question of whether facial recognition results should qualify as *Brady* material.

Despite the thousands of criminal cases in which facial recognition is currently being used,[108] *Lynch v. State* is the only case that has attempted to litigate these *Brady* issues.[109] While it is possible that some disclosure of facial recognition is currently taking place, most cases have remained under the radar,[110] likely because defense counsel were not aware that facial recognition was used in their clients' cases.[111] The lack of cases litigating these *Brady* issues suggests that defendants are consistently being denied access to such information.[112] Notwithstanding the fact that FACES, created by the Pinellas County Sheriff's Office, runs eight thousand monthly facial recognition searches,[113] the Pinellas County Public Defender reports that they have never received facial recognition information as part of *Brady* disclosure.[114] Consequently, it appears that defendants whose cases involve the use of facial recognition software are, perhaps unknowingly, being denied their due process rights.[115]

---

105. *Id.*

106. *Id.*

107. The Florida Supreme Court denied the petition for discretionary review because there is no conflict among Florida district courts. Lynch v. State, No. SC19-298, 2019 Fla. LEXIS 1300, at *1 (July 19, 2019).

108. GAO REPORT, *supra* note 18; Vickie Chachere, *Biometrics Used to Detect Criminals at Super Bowl*, ABC NEWS (Jan. 7, 2006), http://abcnews.go.com/Technology/story?id=98871 [http://perma.cc/Y4FR-F6GF] (discussing the use of facial recognition in criminal investigations); Mich. State Univ., *Facial-Recognition Technology Proves Its Mettle*, SCIENCEDAILY (May 24, 2013), www.sciencedaily.com/releases/2013/05/130524142549.htm [http://perma.cc/Y4FR-F6GF] (discussing a study to evaluate the use of facial recognition technology in criminal investigations such as the Boston marathon bombing).

109. Brief for ACLU, *supra* note 7, at 11.

110. *See* IJIS INST., *supra* note 35 (detailing several cases in which facial recognition has been used).

111. Jackson, *supra* note 35, at 16.

112. However, there are plausible alternative explanations to the lack of litigation on this matter. It is possible that defense counsel are deliberately choosing not to litigate these cases (whether because of strategic or resource-related reasons), or that they don't yet know that they could potentially bring such cases.

113. GARVIE ET AL., *supra* note 51, at 2.

114. *Id.* at 59.

115. Brady v. Maryland, 373 U.S. 83, 87 (1963) ("We now hold that the suppression by the prosecution of evidence favorable to an accused upon request

C. *Brady* Disclosure

1. *Brady* Disclosure of Biometric Data

There are meaningful differences between traditional forms of biometric data and facial recognition that suggest facial recognition results and confidence levels should be *Brady* material. A plaintiff must establish three elements to prove a *Brady* violation: "(1) the evidence at issue must be favorable to the accused, either because it is exculpatory or because it is impeaching; (2) the evidence must have been suppressed by the state, either willfully or inadvertently; and (3) prejudice must have ensued."[116]

Test results from DNA and fingerprints found at the crime scene almost always meet these elements.[117] While defendants generally receive access to *Brady* material for DNA and fingerprint results, that is not the case for facial recognition results.[118] There are, however, differences between these types of biometric data that highlight why facial recognition should be disclosed under *Brady*.[119]

One meaningful difference between fingerprint and facial recognition results is that fingerprint analysts are required to go through

---

violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution.").

116. Strickler v. Greene, 527 U.S. 263, 281–82 (1999).

117. For example, Jerry Watkins was awarded relief on a *Brady* claim regarding suppressed police reports that supported a theory of third-party guilt. Watkins v. Miller, 92 F. Supp. 2d 824, 827 (S.D. Ind. 2000). In 2006, a Massachusetts District Court held that while "*Brady*'s holding specifically contemplated evidence of known exculpatory value, its central premise has been adapted to evidence of uncertain exculpatory value, such as the untested DNA evidence in this case." Wade v. Brady, 460 F. Supp. 2d 226, 245 (D. Mass. 2006); *see also* United States v. DeLeon, No. CR 15-4268 JB, 2017 U.S. Dist. LEXIS 17811, at *180 (D.N.M. Feb. 8, 2017) ("DNA information can be exculpatory material under *Brady*."). Furthermore, in 2001, the Seventh Circuit Court of Appeals concluded that withholding information that showed the plaintiff's fingerprints did not match those at the crime scene was a *Brady* violation. The court found that such material was exculpatory information used to identify the defendant. Newsome v. McCabe, 256 F.3d 747, 751–52 (7th Cir. 2001) (finding that *Brady* established that officers could not withhold information that the plaintiff's fingerprints did not match those at the crime scene).

118. Mitchell v. Sharp, No. 16–6258, 2019 U.S. App. LEXIS 36563, at *1–2 (10th Cir. 2019); Buffey v. Ballard, 782 S.E.2d 204, 221 (W. Va. 2015); *see also Advancing Justice Through DNA Technology: Using DNA to Solve Crimes*, DEP'T OF JUST. (Mar. 7, 2017), https://www.justice.gov/archives/ag/advancing-justice-through-dna-technology-using-dna-solve-crimes [https://perma.cc/KQ2T-JKJ7] (suggesting that changes in federal and state DNA analysis systems are needed).

119. Brief for ACLU, *supra* note 7; Tashea, *supra* note 23 (discussing *Brady* implications of facial recognition).

rigorous training.[120] Many agencies require fingerprint examiners to have a four-year degree in a related field in addition to certification by the International Association for Identification.[121] Additionally, two separate fingerprint examiners review the potential matches before making a final determination.[122] Currently, for facial recognition analysis, there are no national training requirements—training requirements vary widely by law enforcement agency, and some law enforcement receive no training at all on how to conduct facial recognition analyses.[123]

Similar to fingerprint analysts, but strikingly different from their facial recognition counterparts, DNA analysts are required to meet continuing education requirements stipulated by the FBI's Quality Assurance Standards.[124] Furthermore, despite being used in similar ways, the national DNA database, authorized by statute, is highly regulated, while facial recognition databases are not.[125] There is no congressional act overseeing the use of facial recognition.[126] DNA databases also have strict data requirements about what DNA records can be submitted,[127] but no such requirements exist for facial recognition.[128]

Even with relatively high levels of regulation and accuracy, the overwhelming majority of courts have found that biometric data, including

---

120. NAT'L FORENSIC SCI. TECH. CTR., A SIMPLIFIED GUIDE TO FINGERPRINT ANALYSIS (2013), http://www.forensicsciencesimplified.org/prints/how.html [https://perma.cc/3725-H8D7].

121. *Id.*

122. *Id.*

123. GARVIE ET AL., *supra* note 51, at 3.

124. FBI, QUALITY ASSURANCE STANDARDS FOR FORENSIC DNA TESTING LABORATORIES 3, 9–10 (2011), https://federaldefendersny.org/pdfs/FBI%20QAS.pdf [https://perma.cc/93QX-GRMX].

125. The largest such DNA database is CODIS, run by the FBI. *CODIS—NDIS Statistics*, *supra* note 58. CODIS contains over 14 million DNA profiles contributed by federal, state, and local participating forensic laboratories. *Id.* All U.S. states and territories participate through the National DNA Index System (NDIS), which is part of CODIS and authorized by statute. *Frequently Asked Questions on CODIS and NDIS*, *supra* note 58. CODIS and NDIS require that the DNA data is generated by an accredited laboratory, the DNA data must be generated in accordance with the FBI Director's Quality Assurance Standards, and the DNA data must meet minimum CODIS Core Loci requirements (meaning the specific physical location of a gene on a chromosome). *Id.*; *Locus*, NAT'L HUM. GENOME RSCH. INST., https://www.genome.gov/genetics-glossary/Locus [https://perma.cc/RU4K-PD9T].

126. Olivia Solon, *Facial Recognition Bill Would Ban Use by Federal Law Enforcement*, NBC NEWS (June 25, 2020), https://www.nbcnews.com/tech/security/2-democratic-senators-propose-ban-use-facial-recognition-federal-law-n1232128 [https://perma.cc/CSE6-5FLE].

127. *Frequently Asked Questions on CODIS and NDIS*, *supra* note 58.

128. *Supra* Section I.A.

DNA and fingerprint analysis results, qualify as *Brady* material, due to their exculpatory nature.[129] Meanwhile, though facial recognition is much less regulated and has lower rates of accuracy,[130] no court has ruled that facial recognition results and confidence levels should qualify as *Brady* material.[131]

2. *Brady*'s Applicability to Investigative Tools

An important question is whether it matters, for purposes of *Brady*, that facial recognition is currently used for investigative leads and not as the sole basis to establish probable cause for an arrest or as the basis for lay or expert testimony at trial.[132] The fact that facial recognition is not yet (at least publicly[133]) used on its own to establish probable cause is not determinative because courts have found that *Brady* applies to material that can lead to probable cause, not only material that establishes probable cause.[134] Courts have reasoned that information that is "both favorable and of such importance that it can be said to be material to the outcome of a probable cause determination" may cast doubt on the strength of the prosecutor's case and therefore must be disclosed.[135]

Similarly, most jurisdictions mandate disclosure of exculpatory information that can lead to admissible evidence, even if the exculpatory

---

129. While some discovery rules require the disclosure of forensic testing, courts generally analyze the disclosure of forensic testing under *Brady*. *See* MICKENBERG, *supra* note 85, at 8; *Brady Disclosure Requirements*, *supra* note 85 (discussing the *Brady* implications of biometric data); Mitchell v. Sharp, No. 16-6258, 2019 U.S. App. LEXIS 36563, at *1–2 (10th Cir. Dec. 10, 2019) (discussing exculpatory DNA evidence).

130. *See* GROTHER ET AL., *supra* note 32; *see also supra* note 63 (discussing inaccuracies in facial recognition for women, young people, and people of color).

131. Brief for ACLU, *supra* note 7, at 9.

132. Hamann & Smith, *supra* note 29. *But see supra* Section I.D (discussing instances in which facial recognition has been used to establish probable cause).

133. *See supra* Section I.D.

134. *See* United States v. Agurs, 427 U.S. 97, 98 (1976); Giglio v. United States, 405 U.S. 150, 151 (1972); Molnar v. Care House, 574 F. Supp. 2d 772, 794–95 (E.D. Mich. 2008); *see also* Wright v. Hopper, 169 F.3d 695, 703 (11th Cir. 1999) ("Inadmissible evidence may be material if the evidence would have led to admissible evidence."); Spence v. Johnson, 80 F.3d 989, 1005 n.14 (5th Cir. 1996) ("Inadmissible evidence may be material under *Brady*.").

135. Bridgeforth v. Super. Ct., 154 Cal. Rptr. 3d 528, 538 (Cal. Ct. App. 2013); *see also* Ellsworth v. Warden, 333 F.3d 1, 5 (1st Cir. 2003) ("We think it plain that evidence itself inadmissible *could* be so promising a lead to strong exculpatory evidence that there could be no justification for withholding it.") (emphasis in original); Coleman v. Calderon, 150 F.3d 1105, 1116 (9th Cir. [1998]) ("To be material [under *Brady*], evidence must be admissible or lead to admissible evidence."), *rev'd on other grounds*, 525 U.S. 141, 142 (1998).

information is not admissible in its current form.[136] Since the Supreme Court's decision in *Wood v. Bartholomew*, which held that a *Brady* violation occurs when the disclosure of evidence makes it "reasonably likely" that a different result would have been obtained at trial,[137] the First, Sixth, Eighth, Eleventh, and D.C. Circuits have all held that *Brady* violations can occur when inadmissible evidence leads to admissible evidence.[138] Similarly, the Fifth Circuit has held that *Brady* violations can occur when inadmissible evidence would likely affect the outcome of the trial.[139] Each court has concluded that where the disclosure creates a reasonable probability of altering the verdict, the inadmissible evidence is material and disclosure is therefore required.[140]

Despite the due process implications pertaining to favorable and material information, defendants are not receiving access to such information in the context of facial recognition.[141] Courts should apply the

---

136. Henness v. Bagley, 644 F.3d 308, 325 (6th Cir. 2011) (considering inadmissible hearsay evidence when determining if a *Brady* violation occurred, and ultimately holding that the habeas petitioner was not prejudiced because he failed to establish that the inadmissible evidence could have led to the discovery of admissible material evidence), *reh'g denied*, No. 07-4479, 2011 U.S. App. LEXIS 18549 (6th Cir. 2011); *Ellsworth*, 333 F.3d at 5 (discussing the underlying policy of *Brady* and noting that "evidence itself inadmissible *could* be so promising a lead to strong exculpatory evidence that there could be no justification for withholding it" (emphasis in original)); Bradley v. Nagle, 212 F.3d 559, 566–67 (11th Cir. 2000) (discussing a similar theory); Madsen v. Dormire, 137 F.3d 602, 604 (8th Cir. 1998) (finding that alleged impeachment evidence was immaterial because it would not have changed the trial's outcome); Sellers v. Estelle, 651 F.2d 1074, 1077 (5th Cir. 1981) (finding exculpatory evidence in the form of inadmissible hearsay to be *Brady* material).

137. Wood v. Bartholomew, 516 U.S. 1, 6–7 (1995).

138. *See, e.g.*, *Henness*, 644 F.3d at 308; *Ellsworth*, 333 F.3d at 1; *Bradley*, 212 F.3d at 559; *Madsen*, 137 F.3d at 602; United States v. Derr, 990 F.2d 1330, 1335-36 (D.C. Cir. 1993), *abrogated on other grounds by* United States v. Bailey, 36 F.3d 106 (D.C. Cir. 1994) (en banc), *rev'd*, 516 U.S. 137 (1994) (articulating that non-disclosure of inadmissible evidence leading to the discovery of admissible evidence that could have resulted in a different result at trial would be a *Brady* violation), *superseded by statute*, 18 U.S.C. § 924 (2006).

139. United States v. Lee, 88 F. App'x 682, 685 (5th Cir. 2004) (per curiam).

140. Abigail B. Scott, *No Secrets Allowed: A Prosecutor's Obligation to Disclose Inadmissible Evidence*, 61 CATH. U. L. REV. 867, 887–89 (2012).

141. *See* GARVIE ET AL., *supra* note 51 (describing how earlier research found that in the fifteen years the Pinellas County Sheriff's Office had been using facial recognition technology, the Public Defender's Office for the region had never received information about the technology as part of *Brady* disclosure); *see* Reply Brief of Petitioner-Appellant at 7, Lynch v. State, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018) ("It was there [during depositions] that the defense found out that [police analyst] Tenah used a biometric facial recognition program to identify Appellant. Up until then the State had failed to disclose that information.").

conclusions of the First, Sixth, Eighth, Eleventh, and D.C. Circuits to the facial recognition context and find that facial recognition results and confidence information must be provided to defendants under *Brady*, regardless of the admissibility of that evidence or whether it was used to establish probable cause, as long as the information is material and exculpatory.

3. *Brady* Materiality Standard and Facial Recognition

Under the *Kyles* materiality standard, which was affirmed in the Supreme Court's most recent opinion on the issue of materiality,[142] *Brady* demands the pretrial disclosure of facial recognition confidence scores and alternative matches:[143]

> The question is not whether the defendant would more likely than not have received a different verdict with the evidence, but whether in its absence he received a fair trial, understood as a trial resulting in a verdict worthy of confidence. A reasonable probability of a different result is accordingly shown when the government's evidentiary suppression undermines confidence in the outcome of the trial.[144]

In *Kyles*, prosecutors withheld information relating to inconsistent eyewitness identification statements and license plate numbers from the crime scene that did not match the defendant's alleged license plate.[145] The Court found that the inconsistent eyewitness statements and the information pertaining to the license plates were *Brady* material, and the prosecution's lack of disclosure merited reversal.[146] The Court reasoned that the defense could have used that information to "attack[] the reliability of the investigation in failing even to consider [an alternate suspect's] possible guilt."[147] The Court further concluded that the government's suppression undermined confidence in the outcome of the trial because "disclosure of the suppressed evidence to competent counsel would have made a different result reasonably probable."[148]

---

142. Turner v. United States, 137 S. Ct. 1885, 1893 (2017) (finding that "[a] reasonable probability of a different result" is one in which the suppressed evidence "undermines confidence in the outcome of the trial" (internal citations omitted)).

143. *See infra* Section II.C.4 (discussing exceptions).

144. Kyles v. Whitley, 514 U.S. 419, 434 (1995) (internal citations omitted).

145. *Id.* at 428–30.

146. *Id.* at 453–54.

147. *Id.* at 446.

148. *Id.* at 441.

Confidence ratings and alternative matches provided by facial recognition software can undermine the confidence in a conviction and should be provided to defendants similarly to material undermining the credibility of a witness.[149] Regarding confidence ratings, in *Lynch*, facial recognition identified Lynch and several other people in its list of results.[150] All of the results had one-star confidence levels.[151] If a human witness identified, with similar confidence, several other people as possible suspects, that information would unquestionably have qualified as *Brady* material had that witness testified at trial.[152]

Similarly, if a testifying witness expresses a low level of confidence in an eyewitness identification, such information would be *Brady* material.[153] The prosecutor would have to disclose information about the lack of certainty to the defense.[154] In-court witnesses providing confidence information is analogous to facial recognition confidence scores. If it is *Brady* information when a human witness informs law enforcement of her lack of certainty, it should be *Brady* information when facial recognition does, too.

The next step in this analysis requires considering that facial recognition results may lead an eyewitness to identify the defendant, but a

---

149. Wearry v. Cain, 136 S. Ct. 1002, 1004 (2016).

150. Brief for ACLU, *supra* note 7, at 3.

151. *Id.*

152. *See* Floyd v. State, 902 So. 2d 775 (Fla. 2005) (finding witness interviews that indicated an alternative perpetrator was *Brady* material); DiSimone v. Phillips, 461 F.3d 181, 195–97 (2d Cir. 2006) (finding a *Brady* violation because an exculpatory statement would have allowed the defense to investigate another party's involvement); White v. Helling, 194 F.3d 937, 946 (8th Cir. 1999) (finding a *Brady* violation in a murder case because the government did not disclose that its chief eyewitness had originally identified someone else); Rogers v. State, 782 So. 2d 373, 383–84 (Fla. 2001) (finding that undisclosed police reports were "bedrock *Brady* materials" as they "could have been used to show that another person" committed the crime, as reflected by the many witness descriptions matching an alternate suspect).

153. *See* Jacobs v. Singletary, 952 F.2d 1282, 1288 (11th Cir. 1992) (finding that an undisclosed report revealing that a witness was "uncertain" and "unsure" about certain facts undermined his testimony and constituted *Brady* material).

154. For example, imagine a scenario in which an eyewitness viewing a photo array points to the defendant and says, "I think it was this person, but I'm not sure." *See, e.g.*, Boyette v. Lefevre, 246 F.3d 76, 91 (2d Cir. 2001) (finding a witness statement about the uncertainty of the identity of her attacker to be "classic *Brady* material"); *Jacobs*, 952 F.2d at 1288 (finding a *Brady* violation when the state withheld a polygraph report about an eyewitness's lack of certainty about what he saw); Conley v. United States, 332 F. Supp. 2d 302, 315–16 (D. Mass. 2004), *aff'd*, 415 F.3d 183 (1st Cir. 2005) (finding a *Brady* violation when prosecution withheld a memo stating that witness was uncertain of his recollection of events).

fallible process would have led to that identification.[155] This can further undermine the confidence in a conviction. Even if the initial facial recognition results serve only as an investigative lead, eyewitness identifications that confirm the identity of a match would form the foundation of the investigation and, in many cases, would serve to establish probable cause to make an arrest.[156] Given the issues with facial recognition accuracy and eyewitness identifications, however, the identity of the suspect may be wrong.[157] This issue would likely go undetected and would result in the investigation and possibly conviction of an innocent person.[158]

Improper handling of the alternate matches provided by facial recognition software can similarly impact an investigation. Consider a scenario in which a testifying eyewitness viewing a police lineup pointed to three of the five people in the lineup, the defendant and two fillers, and then says, "It was one of these three people." The prosecutor would have to disclose this information.[159] When facial recognition provides multiple results, the software is doing the same, identifying multiple people. If it is *Brady* information when a human witness identifies multiple suspects, it should be *Brady* information when facial recognition does the same.

Moreover, investigations that focus on a suspect who was identified by facial recognition may suffer from confirmation bias and tunnel vision. These issues can occur when the testifying investigator, after using facial recognition to identify the defendant, ignores or inadvertently suppresses evidence that points away from the defendant.[160] Tunnel vision

---

155. *See supra* Section I.C (describing the accuracy of facial recognition); Section I.E (discussing issues with eyewitness identification).

156. Hamann & Smith, *supra* note 29; Valentino-DeVries, *supra* note 68 (discussing instances where facial recognition was the primary basis for an arrest).

157. *See supra* Section I.C (describing the accuracy of facial recognition); Section I.D (discussing issues with eyewitness identification).

158. INNOCENCE PROJECT, *supra* note 71.

159. *See, e.g.*, *Boyette*, 246 F.3d at 91 (finding that documents were *Brady* material because they could have helped the defense suggest an alternative perpetrator); United States v. Robinson, 39 F.3d 1115, 1118 (10th Cir. 1994) (overturning a conviction where the prosecution did not disclose that eyewitness said the perpetrator "may" have had characteristics tending to match the co-defendant).

160. A number of sources discuss the dangerous effects of confirmation bias and feedback on the accuracy of witness identification. *See* James R. Acker & Catherine L. Bonventre, *Perspective: Protecting the Innocent in New York: Moving Beyond Changing Only Their Names*, 73 ALB. L. REV. 1245, 1271–72 (2010); *see also id.* at 1285–86 (discussing the bias effects of tunnel vision); Richard A. Wise et al., *A Survey of Defense Attorneys' Knowledge and Beliefs About Eyewitness Testimony*, 31 CHAMPION 18, 18, 20 (2007) (discussing factors that can influence an eyewitness' confidence); Jacqueline McMurtrie, *The Role of the Social Sciences in Preventing Wrongful Convictions*, 42 AM. CRIM. L. REV. 1271, 1277–78 (2005) (discussing that an eyewitness' confidence does not

can exacerbate due process concerns as there could be exculpatory evidence indicating alternative perpetrators, which would "undermine confidence in the outcome of the trial."[161] Ultimately, then, not disclosing evidence of alternative perpetrators would constitute a *Brady* violation.[162] Overall, courts have found that *Brady* material includes any information that links someone other than the defendant to the crime.[163] *Brady* should therefore apply to alternative matches and confidence levels provided by facial recognition, and that information should be turned over to defendants.

---

correlate with an eyewitness' accuracy); Amy L. Bradfield et al., *The Damaging Effect of Confirming Feedback on the Relation Between Eyewitness Certainty and Identification Accuracy*, 87 J. APPLIED PSYCH. 112, 112 (2002) (identifying ways in which eyewitness confidence can be impacted); Gary L. Wells & Amy L. Bradfield, *"Good, You Identified the Suspect": Feedback to Eyewitnesses Distorts Their Reports of the Witnessing Experience*, 83 J. APPLIED PSYCH. 360, 361 (1998) (discussing how feedback to eyewitnesses distort their accuracy); John S. Shaw III & Kimberly A. McClure, *Repeated Post Event Questioning Can Lead to Elevated Levels of Eyewitness Confidence*, 20 L. & HUM. BEHAV. 629 (1996) (discussing the negative impact of postevent questioning on eyewitness' confidence).

161. *Kyles,* 514 U.S. at 434.

162. *Brady*, 373 U.S. at 87.

163. *See* United States v. Jernigan, 492 F.3d 1050, 1053 (9th Cir. 2007) (finding a *Brady* violation where prosecution failed to "disclos[e] the existence of a phenotypically similar bank robber who had been robbing banks in the same area after Jernigan's incarceration"); Trammell v. McKune, 485 F.3d 546, 551–52 (10th Cir. 2007) (finding a *Brady* violation where prosecution failed to disclose gas station receipts that supported defendant's trial theory linking another person to the crime); Jamison v. Collins, 291 F.3d 380, 389 (6th Cir. 2002) (finding a *Brady* violation because prosecution failed to disclose "positive identification of different suspects by an eyewitness to the crime"); DiLosa v. Cain, 279 F.3d 259, 265 (5th Cir. 2002) (finding a *Brady* violation where the prosecution failed to disclose hair samples, fingerprints, and statements of three witnesses which could undermine confidence in the verdict); Clemmons v. Delo, 124 F.3d 944, 947, 952 (8th Cir. 1997) (finding a *Brady* violation when the state withheld internal prison communication stating that another inmate had observed a different person commit the stabbing); Miller v. Angliker, 848 F.2d 1312, 1321–23 (2d Cir. 1988) (finding that the state withheld significant evidence of investigation into the guilt of another, which warranted reversal even though petitioner had chosen, without that exculpatory information, to plead not guilty by reason of insanity); Bowen v. Maynard, 799 F.2d 593, 612 (10th Cir. 1986) (granting habeas relief because withheld evidence regarding a different suspect created a "reasonable doubt" and "in the hands of the defense, it could have been used to uncover other leads and defense theories and to discredit the police investigation of the murders"); *cf*. Winfield v. United States, 676 A.2d 1, 4 (D.C. 1996) (en banc) (finding evidence showing reasonable possibility of a third party perpetrator is relevant and admissible at trial).

4. *Brady* and the Reliability of an Investigation

Had the defense known about the use of facial recognition in Lynch's case, counsel could have raised questions about the reliability of the investigation under the *Kyles* standard.[164] The FACES analyst expressed that she did not know how FACES worked and, further, that she was unaware there was a range of possible confidence ratings.[165] Additionally, the officers conducting the investigation testified that they had accepted the analyst's suggestion of Lynch's identity without further investigation, even though FACES produced several alternative matches, each of which had the same low confidence rating.[166]

The investigation in *Lynch* appears to have been even less robust than the investigation that occurred in *Kyles*.[167] The same reasoning should therefore apply to *Lynch* and other cases involving facial recognition: if the defense could have used that information to "attack[] the reliability of the investigation in failing even to consider [an alternate suspect's] possible guilt,"[168] it must be turned over. As Jake Laperruque, Senior Counsel at the Constitutional Project, stated:

> Without knowing that facial recognition was used and the details, it's impossible for defendants to know if its use in advancing an investigation was proper. It's the equivalent of police basing their investigation on an eyewitness account, but then not letting the defendant know the witness was used, or if what they saw was from 5 or 500 feet away.[169]

There are circumstances when materiality will not be met in this context, such as when the individuals in the alternative matches provided by facial recognition could not possibly have committed the crime in question (for example, because of incarceration or death). But as long as the confidence levels of a match or other possible matches could "attack[] the reliability of the investigation in failing even to consider [an alternate suspect's] possible guilt"[170] or "'undermine confidence' in the verdict,"[171] defendants should have the chance to review other possible matches and assess the associated confidence scores. To address these concerns, facial recognition results and confidence scores must be disclosed.

---

164. *Kyles,* 514 U.S. at 446.
165. Brief for ACLU, *supra* note 7, at 20.
166. *Id.* at 3, 20.
167. *Kyles*, 514 U.S. at 446.
168. *Id.*
169. Mak, *supra* note 68.
170. *Kyles*, 514 U.S. at 446.
171. Wearry v. Cain, 136 S. Ct. 1002, 1006 (2016).

III. RECOMMENDATIONS FOR THE FAIR USE OF FACIAL RECOGNITION IN CRIMINAL CASES

Defendants face meaningful barriers to challenging the use of facial recognition results. Since results are ultimately in the hands of law enforcement, prosecutors should play a role in ensuring that defendants receive access to exculpatory information. Furthermore, it can be difficult to monitor the discretionary application of *Brady*.[172] Thus, this Part argues that courts, law enforcement agencies, and legislatures must make changes to ensure the proper and beneficial use of facial recognition. Section III.A argues that courts should take an active role in ensuring that facial recognition results are provided as part of *Brady* disclosure by applying the *Kyles* standard of materiality.[173] Section III.B suggests that law enforcement should adopt new guidelines for eyewitness identifications. Section III.C suggests that legislative bodies should create regulations to ensure minimum levels of accuracy and proper use of facial recognition. Only with these advancements can facial recognition be used in a fair and beneficial way.

A. Courts' Role in Requiring *Brady* Disclosure

Courts must play a role in ensuring defendants receive exculpatory material in the facial recognition context. Unfortunately, it has been

---

172. The requirement that prosecutors turn over evidence that is favorable to the defendant requires good-faith judgment on the part of the prosecutor to determine what evidence is favorable or material. Brady v. Maryland, 373 U.S. 83, 87 (1963). Prosecutors are permitted to exercise discretion in assessing the value of evidence, but they should resolve any doubts in favor of disclosure. *See* People v. Fein, 272 N.Y.S. 2d 753, 759 (1966); Bennett L. Gershman, *Between* Brady *Discretion and* Brady *Misconduct*, 123 DICK. L. REV. 661, 670 (2019). That said, prosecutors are not required to seek out evidence for the defense, and since criminal cases are adversarial in nature, prosecutors are not required to disclose evidence that defense lawyers could obtain with reasonable diligence. United States v. Marrero, 904 F.2d 251, 261 (5th Cir. 1990) ("[*Brady*] does not place any burden upon the government to conduct a defendant's investigation or assist in the presentation of the defense's case."); In re Littlefield, 851 P.2d 42, 51 (Cal. 1993) ("The prosecution has no general duty to seek out, obtain, and disclose all evidence that might be beneficial to the defense."); *see also* United States v. Georgiou, 777 F.3d 125, 141 (3d Cir. 2015) (finding that *Brady* does not require the government to provide defendants with evidence they could obtain from other sources by exercising reasonable diligence). No matter how competent a defense lawyer is, though, she will not be able to obtain the results of a facial recognition search, especially if she is not even made aware that such search was conducted.

173. *See* Jones, *supra* note 95; United States v. Hykes, No. CR 15-4299 JB, 2016 WL 1730125, at *18 (D.N.M. Apr. 11, 2016) (discussing various checks that courts have on prosecutors to ensure proper *Brady* disclosure).

noted that "violations of *Brady* are the most recurring and pervasive of all constitutional procedural violations."[174] Furthermore, when the Innocence Project examined DNA exonerations, 37% of the cases "involved the suppression of exculpatory evidence."[175] Despite the scope of *Brady* non-compliance, legal scholars have noted that courts have taken few steps to improve *Brady* disclosure.[176]

While the duty of *Brady* disclosure rests with the prosecution, the *Brady* doctrine has become so complex that "it is virtually impossible to identify clear and consistent norms of compliance by prosecutors as to what evidence is required to be disclosed, when it must be disclosed, and permissible reasons for noncompliance."[177] Moreover, even if prosecutors were to ask their law enforcement partners for *Brady* material, law enforcement agencies do not currently have policies regarding the disclosure of facial recognition search results.[178] The government is not required to provide courts with an inventory of evidence or of what has been disclosed,[179] but judges are in an ideal position to oversee compliance with *Brady*.[180] While some may suggest that it is difficult for courts to monitor discretionary disclosure, if courts were to apply the *Kyles* materiality standard, prosecutors will have articulable guidelines for disclosure, thereby alleviating the burden on courts.

---

174. Bennett L. Gershman, *Litigating* Brady v. Maryland*: Games Prosecutors Play*, 57 CASE W. RES. L. REV. 531, 533 (2007).

175. *See* Cynthia E. Jones, *A Reason to Doubt: The Suppression of Evidence and the Inference of Innocence*, 100 J. CRIM. L. & CRIMINOLOGY 415, 428–31 (2010) (discussing *Brady* violations in death penalty and wrongful convictions cases); Peter A. Joy, *The Relationship Between Prosecutorial Misconduct and Wrongful Convictions: Shaping Remedies for a Broken System*, 2006 WIS. L. REV 399, 403 (2006) (discussing the impact of prosecutorial misconduct on wrongful convictions).

176. Some courts have taken steps to improve this. *See* Press Release, N.Y. State Unified Ct. Sys., Chief Judge DiFiore Announces Implementation of New Measure Aimed at Enhancing the Delivery of Justice in Criminal Cases, at 1 (Nov. 8, 2017), http://www.nycourts.gov/PRESS/PDFs/PR17_17.pdf [https://perma.cc/6P7X-H4CN]; *see also* LAURA L. HOOPER ET AL., FED. JUDICIAL CTR., TREATMENT OF *BRADY V. MARYLAND* MATERIAL IN UNITED STATES DISTRICT AND STATE COURTS' RULES, ORDERS, AND POLICIES: REPORT TO THE ADVISORY COMMITTEE ON CRIMINAL RULES OF THE JUDICIAL CONFERENCE OF THE UNITED STATES 4 (2004), https://www.uscourts.gov/sites/default/files/bradymat_1.pdf [https://perma.cc/GFV6-XDZX] (discussing codification of *Brady* in state criminal procedure rules).

177. Gershman, *supra* note 174, at 534.

178. *See* GARVIE ET AL., *supra* note 51 (describing earlier research which found that in the fifteen years the Pinellas County Sheriff's Office had been using facial recognition technology, the Public Defender's Office for the region had never received information about the technology as part of *Brady* disclosure).

179. Jones, *Here Comes the Judge*, *supra* note 95, at 96–97.

180. *Id.* at 110.

Several courts have already followed the *Kyles* standard, which was affirmed in the Court's recent decision in *Turner v. United States*,[181] for other types of discovery.[182] Adopting the *Kyles* standard will ensure that defendants are given access to facial recognition results, since facial recognition confidence scores and alternative matches can "undermine[] confidence in the outcome of the trial."[183] As previously mentioned, in *Kyles*, the Court reasoned that the defense could have used information to "attack[] the reliability of the investigation in failing even to consider [an alternate suspect's] possible guilt."[184] In cases in which the identification of the defendant is in question, facial recognition results and confidence scores can jeopardize the reliability of an investigation due to the failure to consider an alternative suspect.

Additionally, the Court determined that materiality applies to information that can "affect[] the judgment of the jury."[185] Both facial recognition confidence scores and results can affect the jury's judgment. First, the jury can determine that the unreliability of a low-confidence identification made by facial recognition software may undercut the reliability of the prosecution's proof at trial. Alternatively, the jury can decide that the defendant visually resembled several other individuals, any of whom could have been the perpetrator. Either way, this information may alter the outcome of the proceeding.[186] Therefore, because they are material under the *Kyles* standard and potentially exculpatory, facial recognition confidence scores and results would qualify as *Brady* material.[187]

Critics may argue that prosecutors will not always have to disclose facial recognition results because such results are not always material.[188]

---

181. *Turner*, 137 S. Ct. at 1893; *see also supra* Section II.C.3 (discussing the *Kyles* standard).

182. Floyd v. Vannoy, 894 F.3d 143, 165–66 (5th Cir. 2018); McCormick v. Parker, 821 F.3d 1240, 1248 (10th Cir. 2016); Rivera v. Guevara, 319 F. Supp. 3d 1004, 1044–45 (N.D. Ill. 2018); United States v. McClellon, 260 F. Supp. 3d 880, 886–87 (E.D. Mich. 2017); Kargbo v. Warden, N.H. State Prison, No. 15-cv-315-PB, 2018 U.S. Dist. LEXIS 44456, at *16–18 (D.N.H. 2018); United States v. Lobo, 2017 U.S. Dist. LEXIS 41918, at *10–11 (S.D.N.Y. 2017).

183. *Kyles,* 514 U.S. at 434 (citation omitted).

184. *Id.* at 446; *see also supra* Section II.C.3 (discussing the *Kyles* standard).

185. Wearry v. Cain, 136 S. Ct. 1002, 1006 (2016) (citation omitted); *see Kyles*, 514 U.S. at 453 ("[T]he question is . . . whether we can be confident that the jury's verdict would have been the same.").

186. Brief for Petitioner at 9, Lynch v. State, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018) ("[I]f there were photographs of other suspects who were possible matches for the drug seller, these photos could have cast doubt upon the identification of Petitioner as the drug seller.").

187. *Wearry*, 136 S. Ct. at 1006; *Kyles*, 514 U.S. at 434.

188. *See supra* Section II.C.3 (discussing materiality).

This Note does not dispute that claim. But in the majority of cases, as long as it was reasonable that another individual listed in the search results was the perpetrator, defendants should have access to the search results and confidence levels to dispute the reliability of the investigation.[189]

Even if one does not accept that *Brady* compels the disclosure of facial recognition results and confidence levels, as Justice Kagan articulated in *Turner*, fairness concerns compel prosecutors to provide expansive disclosure.[190] Still, neither expansive disclosure nor the application of the *Kyles* standard can address all of the problematic issues underlying facial recognition software.

B. New Standards for Eyewitness Identification

To minimize highly consequential human errors, the manual inspection procedures of facial recognition results need to be standardized.[191] As part of this standardization, all law enforcement agencies should be required to adopt the January 2017 Procedures for Conducting Photo Arrays set forth by the U.S. Department of Justice (DOJ).[192] Several of the recommendations, however, must be specifically adapted to the facial recognition context.

First, in addition to the suspected perpetrator, there should be at least five possible matches included in every list of facial recognition results.[193] Second, searches should include the use of blind administrators, whereby neither the officer conducting the facial recognition search nor the officer running the identification procedure is the investigating officer.[194] Third, witnesses viewing the photo array should be required to make a statement of confidence, and that statement should additionally qualify as *Brady* material.[195] Fourth, officers conducting the photo array should make

---

189. *Kyles*, 514 U.S. at 446.

190. *Turner*, 137 S. Ct. at 1897 (Kagan, J., dissenting) ("Constitutional requirements aside, turning over exculpatory materials is a core responsibility of all prosecutors—whose professional interest and obligation is not to win cases but to ensure justice is done.").

191. Anil K. Jain et al., *Face Recognition: Some Challenges in Forensics*, INT'L CONF. ON AUTOMATIC FACE & GESTURE RECOGNITION 726, 728 (2011), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5771338 [https://perma.cc/4DG6-ENXG].

192. Memorandum from Sally Q. Yates to Heads of Dep't L. Enf't Components (Jan. 6, 2017), https://www.justice.gov/archives/opa/press-release/file/923201/download [https://perma.cc/XUS9-FJWH].

193. INNOCENCE PROJECT, *supra* note 71, at 18.

194. Memorandum from Sally Q. Yates, *supra* note 192.

195. *Id.*; *Eyewitness Confidence Can Predict Accuracy of Identification, Researchers Find*, ASS'N FOR PSYCHOL. SCI. (Mar. 31, 2017), https://www.psychologicalscience.org/

it clear to the witness that the perpetrator "may or may not be present" in the photo array.[196] Fifth, witnesses should be assured that the investigation will continue even if they don't make a selection, thereby ensuring that witnesses do not feel pressured to make a selection.[197] Finally, photo arrays using facial recognition results should be shown sequentially to witnesses.[198] Together, these measures may decrease the chance of mistakenly identifying an innocent person.[199]

C. Regulation of Facial Recognition

Several organizations have argued that facial recognition is too dangerous and should be outright banned.[200] This Note does not suggest that law enforcement's use of facial recognition should end. Its use and accuracy, however, must be regulated to ensure the lowest possible level of misidentification. While the technology will continue to develop, regulations can be adopted to harness the beneficial uses of the software while minimizing its risks.[201]

Despite the fact that more than 117 million American adults are included in facial recognition databases across the country, the use of these databases and searches remains unregulated.[202] Notwithstanding the number of individuals implicated in facial recognition searches, no state has passed a law comprehensively regulating facial recognition[203] or governing the type of edits law enforcement can make to probe photographs before searching for matches.[204]

---

observer/eyewitness-confidence-can-predict-accuracy-of-identifications-researchers-find [https://perma.cc/2NUP-HXZQ].

196. *Id.* at 19.

197. *Id.*; Memorandum from Sally Q. Yates, *supra* note 192, at 3–4.

198. INNOCENCE PROJECT, *supra* note 71, at 21.

199. *Id.*

200. Siga Samuel, *Activists Want Congress to Ban Facial Recognition. So They Scanned Lawmakers' Faces*, VOX (Nov. 15, 2019), https://www.vox.com/future-perfect/2019/11/15/20965325/facial-recognition-ban-congress-activism [https://perma.cc/RS34-W52H].

201. Henry Ennis et al., *National Security and Technology Regulation*, DELOITTE (Jul. 12, 2019), https://www2.deloitte.com/us/en/insights/industry/public-sector/national-security-technology-regulation.html [https://perma.cc/J9W9-XTTB].

202. GARVIE ET AL., *supra* note 51. Only two law enforcement agencies currently condition the use of facial recognition on certain levels of accuracy, and only eight agencies have specially-trained personnel review potential matches. *Id.* at 3.

203. *Id.* at 2.

204. Garvie, *supra* note 57; Jackson, *supra* note 35, at 15 (discussing the various editing techniques law enforcement agencies make to photos before running them through facial recognition software).

To address the disparities in facial recognition's use, legislators should pass a law to regulate law enforcement's use of facial recognition, parts of which should be modeled after the DNA Identification Act of 1994.[205] Under such a law, the FBI should have authority to establish a national facial recognition index system for law enforcement purposes and to create standards for the quality and use of probe photographs across all law enforcement agencies, similar to NDIS and CODIS.[206]

Specifically, facial recognition software should be required to meet a minimum threshold of accuracy, and there should be regulations on the types of editing allowed.[207] The FBI should partner with NIST to create these standards. Furthermore, Congress should require that all law enforcement facial recognition programs participate in NIST accuracy tests and tests for racially biased error rates and publicly report the results. Law enforcement agencies should be required to disclose information annually and publicly, comparable to the level of disclosure required by the Wiretap Act.[208] This should include the number of facial recognition searches conducted, the crimes that the searches were used to investigate, and the arrests and convictions that resulted from the searches.[209] Lastly, as part of their authority, the FBI should require special training for law enforcement officials who conduct facial recognition searches. This training should include lessons in eyewitness identification as well as the mechanics behind facial recognition, and should be modeled off of training and certification requirements for fingerprint analysts.[210]

If Congress works with the FBI and state and local law enforcement agencies to address the concerns outlined in this Note, facial recognition

---

205. *But see* Schuppe, *supra* note 19 (discussing a bill proposed in the Senate that would limit federal law enforcement use of facial recognition). From 2015 through April 6, 2021, thirteen bills have been introduced that would, in some capacity, address facial recognition. *Legislative Search Results*, CONGRESS.GOV, https://www.congress.gov/search?searchResultViewType=expanded&q=%7B%22source%22:%22legislation%22,%22search%22:%22%5C%22facial+recognition%5C%22%22,%22congress%22:%5B117,116,115,114%5D,%22subject%22:%22Crime+and+Law+Enforcement%22%7D [https://perma.cc/FPX5-PLH6] (providing fourteen results for bills containing the terms "facial recognition").

206. *See supra* Section I.C; *Frequently Asked Questions on CODIS and NDIS*, *supra* note 57 (discussing database input and use standards for NDIS and CODIS).

207. GARVIE ET AL., *supra* note 51.

208. *See* 18 U.S.C. § 2519.

209. GARVIE ET AL., *supra* note 51, at 65 (recommending mandatory, annual disclosure of facial recognition data).

210. *See* Bonsor & Johnson, *supra* note 27; NAT'L FORENSIC SCI. TECH. CTR., *supra* note 120 (discussing training requirements for fingerprint analysts).

has the potential to be safely used as a powerful tool for law enforcement.[211]

CONCLUSION

As law enforcement continues to use facial recognition software,[212] more and more individuals will be at risk of being denied the right to a fair trial.[213] Unless changes are made to recognize facial recognition results and confidence levels as *Brady* material, defendants like Lynch will continue to be deprived of this information. As this Note suggests, law enforcement, judges, and legislators should rethink current standards for facial recognition to ensure that defendants receive access to material that could "undermine confidence" in their verdicts.[214] Without addressing the current lack of regulation of facial recognition both in the courtroom and in criminal investigations, the software is prone to continued misuse, whether by failing to identify the correct suspect or, worse, identifying the wrong individual.

If the tool is used properly, the design is improved upon to effectively control for bias, and the results are properly disclosed, facial recognition could have the potential to be beneficial—criminal defendants could be identified with accuracy, thereby reducing convictions of innocent people.[215] If used improperly, however, it could lead to unjust outcomes. Courts should apply the *Kyles* standard of materiality[216] to ensure facial recognition information qualifies as *Brady* material. Prosecutors and law

---

211. *See, e.g.*, Shanika Gunaratna, *The Tech That Went into Catching the NY, NJ Bombing Suspect*, CBS NEWS (Sept. 19, 2016), www.cbsnews.com/news/tech-that-went-intro-catching-nj-nj-bomb-suspect/ [https://perma.cc/GU3P-N249]; Anthony M. DeStefano, *How Bomb Suspect Ahmad Khan Rahami Was Caught in Just 50 Hours*, NEWSDAY (Sept. 19, 2016), http://www.newsday.com/news/new-york/how-bomb-suspect-ahmad-khan-rahami-wascaught-in-just-50-hours (on file with the *Columbia Human Rights Law Review*) (discussing the effective use of facial recognition in the case of the Boston marathon bombing).

212. *See* Lynch, *supra* note 8.

213. United States v. Bagley, 473 U.S. 667, 674–76 (1985).

214. *See Wearry*, 136 S. Ct. at 1006 (finding that the newly revealed evidence sufficed to undermine confidence in the defendant's conviction).

215. John Dowden, *Facial Recognition in Law Enforcement: Real World Use Cases*, EVIDENCE MAG. (Summer 2018), http://read.nxtbook.com/wordsmith/evidence_technology/summer_2018/index.html#facial_recognition_in_law_enf [https://perma.cc/CMC6-4B6U] (detailing successful uses of facial recognition software to assist law enforcement).

216. *Kyles*, 514 U.S. at 434 ("A 'reasonable probability' of a different result is accordingly shown when the government's evidentiary suppression 'undermines confidence in the outcome of the trial.'" (citing *Bagley*, 473 U.S. at 678)).

enforcement should disclose facial recognition results and confidence levels. Finally, Congress should regulate facial recognition to make sure it is used fairly, beneficially, and accurately. Facial recognition is rapidly becoming a pillar of law enforcement investigations, but if the checks on its use are insufficient, it will implicate innocent people.[217]

217. Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html (on file with the *Columbia Human Rights Law Review*).