2021

Facing Injustice: How Face Recognition Technology May Increase the Incidence of Misidentifications and Wrongful Convictions

Laura M. Moy

FACING INJUSTICE: HOW FACE RECOGNITION TECHNOLOGY MAY INCREASE THE INCIDENCE OF MISIDENTIFICATIONS AND WRONGFUL CONVICTIONS

Laura Moy*

ABSTRACT

Does law enforcement use of face recognition technology paired with eyewitness identifications increase the incidence of wrongful convictions in U.S. criminal law? This Article explores this critical question and posits that the answer may be yes. Facial recognition is frequently used by law enforcement agencies to help generate investigative leads that are then presented to eyewitnesses for positive identification. But erroneous eyewitness accounts are the number one cause of wrongful convictions, and the use of face recognition to generate investigative leads may create the conditions for erroneous eyewitness identifications to take place. This is because face recognition technology is designed to query a large database of faces to find lookalikes, and sometimes an innocent lookalike will resemble a suspect so closely that police may mistakenly select that person as an investigative lead, and an eyewitness may be unable to tell the difference between the lookalike and the actual suspect. This Article explores this possible problem and offers policy recommendations to help address it.

* Associate Professor of Law, Georgetown University Law Center and Director of the Communications & Technology Law Clinic. The author is grateful to Alvaro Bedoya, Barry Friedman, Woodrow Hartzog, Katie Kinsey, Megan Graham, Amanda Levendowski, Jumana Musa, and Nathan Freed Wessler for their helpful comments on a draft of this Article.

INTRODUCTION

Nijeer Parks, of Paterson, New Jersey, had never even set foot in Woodbridge when his grandmother called him in January of 2019 to tell him that the Woodbridge police had a warrant out for his arrest.[1] He got a ride to Woodbridge to clear up what he thought was obviously a mistake, only to find himself arrested, charged with a crime, and held at the county jail for ten days, including four days in intake, isolated from other people.[2] He spent ten months working to clear his name before the charges against him were finally dropped on the night before he was set to go to trial.[3]

Michael Oliver, of Detroit, Michigan, was driving to work in July of 2019 when he was pulled over, arrested, and charged with felony larceny in connection with an incident in which someone else had reached into a car, grabbed someone's phone, and threw it.[4] He was held in police custody for three days before being let go, and the charges were dropped against him two weeks later.[5]

Robert Williams, of Farmington Hills, Michigan, had just arrived home from work in January of 2020 when two Detroit police officers approached him in his driveway and arrested him in front of his wife and two young daughters for a 2018 shoplifting incident in a store that Mr. Williams had only been to once, in 2014.[6] He was detained for thirty hours and forced to sleep on the floor of an overcrowded cell before he was released on a personal bond.[7] The charges were then dropped against him, but he and his family were traumatized by the incident. His daughters took up playing games involving arresting people and have accused Robert of stealing things.[8]

---

[1] Complaint at 2, Parks v. McCormack, No. PAS-L-003672-20, 2020 WL 7773857 (N.J. Sup. Ct. Law Div. filed Nov. 25, 2020) [hereinafter *Parks* Complaint].

[2] *Id.* at 2, 3.

[3] *Id.* at 5; *see also* Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Dec. 29, 2020), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html [https://perma.cc/A5KK-QWJY].

[4] Complaint at 3, 5, Oliver v. Bussa, No. 20-11495, 2020 WL 7658318 (Mich. Cir. Ct. filed Sept. 4, 2020) [hereinafter *Oliver* Complaint].

[5] *Id.* at 5, 6.

[6] Complaint at 2, 3, 28, Williams v. City of Detroit, No. 2:21-cv-10827 (E.D. Mich. filed Apr. 13, 2021) [hereinafter *Williams* Complaint].

[7] *Id.* at 2, 3.

[8] *See id.* at 39, 56; *see also ACLU Calls on Lawmakers to Immediately Stop Law Enforcement Use of Face Recognition Technology*, ACLU (June 24, 2020), https://www.aclu.org

These three cases of mistaken identity followed the same pattern. In all three cases, law enforcement representatives had an image of a perpetrator, used face recognition software to search for people whose faces resembled that image, developed a lead based on the search results, confirmed their lead with the help of an eyewitness identification, then made an arrest.[9] In all three cases, face recognition technology directed law enforcement representatives to the wrong suspect, and eyewitnesses erroneously confirmed the mistaken identification.[10]

This pattern raises an important question: Does law enforcement use of face recognition technology increase the likelihood of erroneous eyewitness identifications, and therefore ultimately of wrongful convictions in U.S. criminal law? This possibility has been hinted at by various scholars, practitioners, and journalists.[11] Others have commented at length about the risk of misidentification by face recognition technology, without delving into use cases that involve both face recognition technology and eyewitness identification.[12] This Article dives deeper into this intersection, exploring the likelihood that the answer to this critical question is yes—that face recognition technology increases the likelihood of misidentification *by eyewitnesses*—and explaining how and why, drawing from factual accounts of how face recognition technology is used and psychological research on how eyewitnesses identify suspects from memory.

/press-releases/man-wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart [https://perma.cc/4S7H-58DB].

[9] *See Oliver* Complaint, *supra* note 4, at 4, 5; *Williams* Complaint, *supra* note 6, at 3, 4–5, Hill, *supra* note 3; ACLU, *supra* note 8.

[10] *See Oliver* Complaint, *supra* note 4, at 4; *Williams* Complaint, *supra* note 6, at 3, 4–5; Hill, *supra* note 3.

[11] *See* Kaitlin Jackson, *Challenging Facial Recognition Software in Criminal Court*, THE CHAMPION 14, 17 (July 2019) ("One argument that attorneys can make is this: the inclusion of a suspect selected by [face recognition software] *unreasonably increased the chance of eye-witness misidentification*.") (emphasis in original); Rebecca Darin Goldberg, Note, *You Can See My Face, Why Can't I? Facial Recognition and* Brady, 5 COLUM. HUM. RTS. L. REV. ONLINE 261, 274–76 (2021), http://blogs.law.columbia.edu/hrlr/files/2021/04/261_Goldberg.pdf [https://perma.cc/7J8K-Q2ZM]; Hill, *supra* note 3.

[12] *See, e.g.*, Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU BLOG (July 26, 2018, 8:00 AM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [https://perma.cc/Z9D2-XUZ7]; Hiawatha Bray, *Mistaken ID: Facial-Recognition Tool Falsely Matches Famous Athletes to Police Mugshots*, BOS. GLOBE (Oct. 21, 2019, 4:35 PM), https://www.bostonglobe.com/business/2019/10/21/athletes-outlaws-the-software-not-sure/lCwfZSCyzlymLzX3NCwasK/story.html [https://perma.cc/2ZME-Y3P2]; Paul Bischoff, *Amazon Face Recognition Falsely Matches 105 US and UK Politicians with Police Mugshots, But Can You Trust Accuracy Claims?*, COMPARITECH (May 28, 2020), https://www.comparitech.com/blog/vpn-privacy/facial-recognition-study/ [https://perma.cc/RAY7-NRCH]; BIG BROTHER WATCH, FACE OFF: THE LAWLESS GROWTH OF FACIAL RECOGNITION IN UK POLICING 25 (2018), https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf.

What happened to Nijeer Parks, Michael Oliver, and Robert Williams likely were not isolated incidents. Face recognition technology is in widespread use by U.S. law enforcement agencies.[13] More than half of U.S. adults are in a law enforcement face recognition database.[14] The exact proportion of the nation's approximately 18,000 law enforcement agencies that use face recognition in some way is unknown, but as of five years ago, was estimated to be at least one-quarter, and may be far greater by now.[15]

Despite being in wide use, this technology is still far from perfect, and current research—as well as the real cases of Mr. Parks, Mr. Oliver, and Mr. Williams—suggest that use of the technology may amplify the risk and incidence of misidentifications and therefore also wrongful convictions. At least four things contribute to this problem and are examined in this Article. First, the use of face recognition technology sometimes inevitably generates lookalike false leads.[16] Second, human analysts sometimes use face recognition systems in ways that diminish the reliability of investigative leads.[17] Third, lookalike false leads confuse eyewitnesses into making misidentifications.[18] And fourth, over time, greater reliance on automated face recognition to generate leads may displace traditional techniques that are less prone to the generation of lookalike false leads.[19] The sum result is that the adoption and use of automated face recognition may lead to the wrongful arrest, prosecution, and conviction of people for crimes they did not commit.

If law enforcement use of automated face recognition facilitates misidentifications and wrongful convictions, policymakers must respond swiftly to address this problem.[20] They should first consider whether it is even possible to prevent face recognition technology from generating lookalike false leads; if not, they should consider prohibiting law enforcement use of face recognition technology altogether. Policymakers should also consider whether, in light of the research, eyewitness identifications of strangers can ever be considered reliable; if not, they should consider adopting a rule requiring corroborating evidence in cases involving eyewitness identification. At a minimum, such a rule should be adopted in cases where face recognition technology has been used.

Policymakers also should adopt rules improving upon eyewitness identification procedures, with or without the use of face recognition technology. Because so many

---

[13] *See* CLARE GARVIE ET AL., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA (2016), https://www.perpetuallineup.org/ [https://perma.cc/SK3C-DK5B].

[14] *Id.* (stating that over 117 million American adults are in law enforcement face recognition networks).

[15] *See id.* at 25.

[16] *See* discussion *infra* Section II.A.

[17] *See* discussion *infra* Section II.B.

[18] *See* discussion *infra* Section II.C.

[19] *See* discussion *infra* Section II.D.

[20] *See* discussion *infra* Part III.

wrongful convictions are based on mistaken eyewitness identifications, advocates have been seeking reforms to eyewitness identification procedures for years, and many jurisdictions have adopted them.[21] But the increasing use of face recognition technology increases the urgency with which these reforms must be passed.

Part I of this Article explains how face recognition is used in conjunction with eyewitness identification in the law enforcement context. Part II explores how and why the growing use of face recognition technology may increase, rather than decrease, misidentifications and therefore wrongful convictions. Part III recommends policy changes that should be considered, including some of the reforms to eyewitness identification procedures that have been advanced by others.

I. SITUATING LAW ENFORCEMENT USE OF FACE RECOGNITION IN CONTEXT

A face recognition "match" is not yet considered evidence of identity for establishing probable cause against an individual or for prosecuting them in court. Instead, face recognition technology typically is used in conjunction with eyewitness identification, and eyewitness identification typically is then used to establish probable cause and support prosecution. This Section discusses how law enforcement agencies in the U.S. typically use face recognition technology as an investigative tool.

A. A Brief Introduction to Law Enforcement Use of Face Recognition on Archival Photographs and Videos

The use of automated face recognition technology by law enforcement agencies is widespread in the United States.[22] It is difficult to estimate exactly how widespread due to the large number of law enforcement agencies—approximately 18,000[23]—and to the fact that agencies often are not transparent about their use of face recognition technology.[24] But a few years ago, researchers at the Center on Privacy & Technology at Georgetown Law submitted public records requests to over one hundred federal, state, and local law enforcement agencies and found that about one-quarter of those that responded said they were already using face recognition technology.[25] That number almost certainly has risen since that time.

Face recognition is used routinely by law enforcement agencies to develop investigative leads from archival (i.e., not live or real-time) photographs and videos.[26]

---

[21] *See Eyewitness Identification Reform*, THE INNOCENCE PROJECT [hereinafter *Eyewitness Identification Reform*], https://innocenceproject.org/eyewitness-identification-reform/ [https://perma.cc/47S3-2QES] (last visited Dec. 13, 2021).

[22] *See* GARVIE ET AL., *supra* note 13, at 24–26.

[23] U.S. DEP'T. OF JUST., NCJ 249681, NATIONAL SOURCES OF LAW ENFORCEMENT EMPLOYMENT DATA 1 (2016).

[24] *See* GARVIE ET AL., *supra* note 13, at 58–59.

[25] *Id.* at 25.

[26] *See* Jackson, *supra* note 11, at 14.

In this application of face recognition, a detective is in possession of a still photograph containing a face that they wish to identify, such as a frame from a security camera that captured an alleged perpetrator at or near the scene of a crime. There are other uses of face recognition technology, such as real-time face recognition analysis performed on live video feeds, but this Article focuses on non-live face recognition used to facilitate eyewitness identification.

Automated face recognition assists law enforcement with putting a name to a face in an image captured by, for example, a street camera, privately owned CCTV camera, or ATM.[27] Identifying a person captured on camera can be a difficult task, especially in a large city. In an analog world, a detective might show a copy of the photograph to people in the area and see if anyone recognizes the person in the photograph, or perhaps perform a labor-intensive manual comparison against mugshots of people believed to have committed similar crimes in the past. Automated face recognition dramatically changes the approach. With the assistance of a computer, a detective can quickly compare the photograph against a database of known faces in search of likely matches.[28] The databases used by law enforcement systems vary, but two common types are those containing mugshots of people who have been previously arrested and photographed upon arrest, and those containing driver's license photos.[29]

When probed with the photo of an unidentified individual, face recognition systems used by law enforcement agencies typically are designed to return "candidate lists" of numerous possible matches from the database, rather than the name and face of a single positive match.[30] For example, the New York Police Department's system returns a list of two hundred candidates in response to each query.[31] Candidate lists generally are provided in a ranked order, with candidates determined by the software to be more similar to the probe photo ranked higher, and those that are less similar ranked lower. Candidate lists often include additional information alongside candidates, which may include "confidence scores" (scores assigned by the software indicating how similar each candidate's photo is to the probe photo), biographical information, or information about prior criminal history.[32]

---

[27] *See NYPD Questions and Answers: Facial Recognition*, N.Y. POLICE DEP'T, https://www1.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page [https://perma.cc/7ZMT-NDJR] (last visited Dec. 13, 2021); GARVIE ET AL., *supra* note 13, at 11.

[28] *See* GARVIE ET AL., *supra* note 13, at 11.

[29] *Id.* at 2–4, 19–20; Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, WASH. POST (July 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/ [https://perma.cc/463P-JW6H].

[30] GARVIE ET AL., *supra* note 13, at 11.

[31] *See Presentation on: Facial Identification Section Overview*, NYPD REAL TIME CRIME CTR. (slides and presenter notes on file with Center on Privacy & Technology at Georgetown Law) [hereinafter NYPD, *Facial Identification*].

[32] *See* Jackson, *supra* note 11, at 20.

Once face recognition software generates a candidate list of possible matches, a law enforcement representative conducts a manual comparison of faces on the list in an attempt to identify a likely match from among the candidates.[33] The person who performs the manual comparison may take other information into account when conducting the comparison, such as the address of each candidate (on the assumption that a candidate who resides near the scene of a crime is more likely to be the person who committed the crime than someone who lives farther away) and each candidate's prior criminal history (on the assumption that a candidate who has been convicted of a similar crime in the past is more likely to be the person who committed the crime than someone who does not have a similar history).[34]

As of the writing of this Article, law enforcement agencies that have spoken on the matter invariably have stated that they do not consider a likely face recognition match to constitute probable cause to make an arrest. Possible face recognition matches are considered to be investigative leads only, and must be corroborated by additional evidence before an arrest can be made. For example, in 2019, an FBI official told the House Oversight Committee, "[t]he FBI's use of facial recognition produces a potential investigative lead and requires investigative follow-up to corroborate the lead before any action is taken."[35] The NYPD patrol guide on face recognition similarly states, "A possible match candidate shall be treated as an investigative lead only. It does not by itself establish probable cause to make an arrest or obtain an arrest or search warrant. Corroborating information must be developed through additional investigation by the assigned investigator."[36] Other departments that have spoken on the matter are in general agreement.[37]

---

[33] *See* NYPD, *Facial Identification*, *supra* note 31.

[34] *See id.* (describing multiple real cases in which the possible match had previous arrests in the vicinity for similar crimes).

[35] *Facial Recognition Technology (Part II): Ensuring Transparency in Government Use: Hearing Before the H. Comm. on Oversight and Reform*, 116th Cong. (2019) (statement of Kimberly J. Del Greco, Deputy Assistant Dir., Crim. Just. Info. Servs., Fed. Bureau Investigation).

[36] N.Y. POLICE DEP'T, PATROL GUIDE: FACIAL RECOGNITION TECHNOLOGY 3 (2020), https://www1.nyc.gov/assets/nypd/downloads/pdf/nypd-facial-recognition-patrol-guide.pdf [https://perma.cc/G49V-E48A].

[37] *See, e.g.,* Jon Schuppe, *How Facial Recognition Became a Routine Policing Tool in America*, NBC NEWS, May 11, 2019, https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251 [https://perma.cc/B354-A3GA] (quoting Rick Sheets, an investigator in Arapahoe County, Colorado); ORLANDO POLICE DEP'T, ORLANDO POLICE DEPARTMENT POLICY AND PROCEDURE: 1147.1, FACIAL RECOGNITION 1 (2021); Nancy Kaffer, *He Was Arrested Because of a Computer Error. Now He Wants to Fix the System.*, DETROIT FREE PRESS (June 24, 2020), https://www.freep.com/story/opinion/columnists/nancy-kaffer/2020/06/24/robert-williams-detroit-police-facial-recognition/3247171001/ [https://perma.cc/3FVS-8BP7] (quoting an official statement from the Detroit Police Department).

B. A Brief Overview of Eyewitness Identification Procedures and Pitfalls

Eyewitness identification refers to when a person who saw another person believed to have committed a crime helps law enforcement to identify the perpetrator. Sometimes the perpetrator is a person known to the eyewitness, and the eyewitness helps law enforcement name and/or locate the known individual, then confirms that the person arrested is, in fact, the person who committed the crime. But oftentimes, the perpetrator is a stranger to the eyewitness. When the perpetrator is not known to the eyewitness, law enforcement representatives develop a lead some other way, then present their suspect to the eyewitness for confirmation that the suspect is the same person who was seen by the eyewitness.[38]

There are two main types of eyewitness identification procedures: showups and lineups.[39] In a showup, a law enforcement representative simply presents the eyewitness with a single suspect and asks them to confirm that this suspect is the right person.[40] In a lineup, the law enforcement representative presents the eyewitness with the suspect alongside several "fillers"—individuals who are not the suspect—and asks the eyewitness to select the person they saw from among the group.[41] A lineup may be "live" or "in person," with the suspect and fillers physically appearing before the witness, typically behind a glass window, or it may be conducted as a "photo lineup," with only a photograph of the suspect presented to the witness alongside photographs of several fillers.[42]

Although eyewitness identification is widely used in the criminal legal process, it is notoriously unreliable. As far back as 1967, the Supreme Court acknowledged that "[t]he vagaries of eyewitness identification are well-known; the annals of criminal law are rife with instances of mistaken identification."[43] And the American Psychological Association, acting as an amicus, has made this point before courts in multiple cases.[44]

Witnesses have imperfect memory and are susceptible to suggestion, so under certain circumstances they may be influenced to identify someone they would not independently recognize.[45] Witnesses are also susceptible to confirmation bias, which may cause the certainty of their identification to increase over time, even following

---

[38] NAT'L RSCH. COUNCIL, IDENTIFYING THE CULPRIT: ASSESSING EYEWITNESS IDENTIFICATION 22 (2014).

[39] Gary L. Wells et al., *Policy and Procedure Recommendations for the Collection and Preservation of Eyewitness Identification Evidence*, 44 L. & HUM. BEHAV. 3, 7 (2020).

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] United States v. Wade, 388 U.S. 218, 228 (1967).

[44] *See generally* Brief of the American Psychological Association as Amicus Curiae Supporting Defendant-Appellant, People v. Boone, 30 N.Y.3d 521 (2017); Brief of the American Psychological Association as Amicus Curiae Supporting Petitioner, Garner v. People, 436 P.3d 1107, *cert. denied sub nom*. Garner v. Colorado, 140 S. Ct. 448 (2019).

[45] *See* NAT'L RSCH. COUNCIL, *supra* note 38, at 15.

initial uncertainty, so that at trial an eyewitness may appear deceptively confident about an identification they were initially uncertain about.[46] Legal scholar Brandon L. Garrett reviewed available information regarding 250 individuals who were wrongfully convicted and later exonerated based on DNA evidence, and found that although eyewitnesses were certain at trial that they had identified the right person, "in 57% of [the available] trial transcripts . . . the witnesses reported they had *not* been certain at the time of the earlier identifications."[47]

Showups are widely understood to be more likely to lead to identification errors than lineups.[48] By their very nature, showups are suggestive.[49] As the Supreme Court acknowledged in 1967, "[t]he practice of showing suspects singly to persons for the purpose of identification, and not as part of a lineup, has been widely condemned."[50] According to one analysis, showups are about two to three times as likely to result in false identification than lineups.[51]

As a general rule, lineups are considered less likely to lead to error than showups, but lineups are far from perfect.[52] There is wide variation in lineup procedures, and there are common deficiencies that can increase the likelihood of an identification error and/or of a witness's confidence regarding an erroneous identification.[53] Three core types of such deficiencies are biased lineups, confirming feedback, and the absence of the culprit.[54] In a biased lineup, the suspect stands out from fillers in the lineup for some reason, increasing the likelihood that an eyewitness will be able to select the suspect even if the eyewitness does not specifically recognize the suspect's face.[55] In confirming feedback, after an eyewitness makes an identification in a lineup, something occurs to increase the eyewitness's confidence regarding their identification and to lead them to believe that they were highly confident all along, even if they were initially uncertain.[56] And in absence of the culprit, the culprit simply is not part of the lineup, thus increasing the likelihood that an eyewitness will erroneously identify an innocent person.[57] Eyewitnesses have been shown to have great difficulty

---

[46] *See* BRANDON L. GARRETT, CONVICTING THE INNOCENT: WHERE CRIMINAL PROSECUTIONS GO WRONG 46–47 (2011).

[47] *Id.* at 49.

[48] *See* Gary Wells, *Eyewitness Identification*, *in* 2 REFORMING CRIMINAL JUSTICE: POLICING 259, 276 (Erik Luna, ed., 2017); Wells et al., *supra* note 39, at 7.

[49] *See* GARRETT, *supra* note 46, at 52; NAT'L RSCH. COUNCIL, *supra* note 38, at 28.

[50] Stovall v. Denno, 388 U.S. 293, 302 (1967).

[51] Jennifer E. Dysart & R. C. L. Lindsay, *Show-up Identifications: Suggestive Technique or Reliable Method?*, *in* THE HANDBOOK OF EYEWITNESS PSYCHOLOGY: VOLUME II: MEMORY FOR PEOPLE 137, 141 (R.C.L. Lindsay et al. eds., 2007).

[52] *See* Wells, *supra* note 48, at 260.

[53] *See* NAT'L RSCH. COUNCIL, *supra* note 38, at 23–26.

[54] Wells, *supra* note 48, at 265–68.

[55] *Id.* at 265.

[56] *Id.* at 265–66. For example, the lineup administrator remarks "good" after the identification is made.

[57] *Id.* at 267.

recognizing when the culprit is not present, even when explicitly told that the culprit may not be in the lineup.[58] As a result, eyewitnesses are likely to select someone from a lineup even when the culprit is absent.[59]

These lineup problems can and do occur together, compounding each other's effects: Even if the culprit is absent from a lineup, an eyewitness may feel pressured to select someone, and due to structural bias in the lineup, may be more likely to select the suspect than a filler.[60] After making the selection, the eyewitness may become more confident in their selection, and appear before a judge and jury expressing great confidence despite their initial uncertainty.[61]

Psychologist and eyewitness identification expert Gary Wells reviewed aggregate data from eleven field studies of identifications in actual cases, representing nearly 7,000 real attempts by eyewitnesses to identify perpetrators from lineups, and found that across those real cases, eyewitnesses picked an innocent filler a staggering 36.8% of the time when they made an identification.[62] Laboratory studies of eyewitness identifications yield similar results: according to one review of ninety-four such studies, when eyewitnesses picked someone out of a lineup in a simulation, they picked a filler 31.5% of the time.[63] In simulations in which the lineup did not include the target individual, eyewitnesses still made a selection 47.9% of the time.[64]

Although lineups can be and sometimes are flawed, these problems are not new and not without solutions. Psychologists have been studying lineups for decades and they, alongside advocates, have long been devising and promoting procedural changes to improve fairness and reduce the incidence of eyewitness identification error.[65] Lineup procedure is not static, and improvements to lineup procedures are constantly being adopted in laws and policies.[66] Among these are several reforms that have been endorsed and promoted by, among others, the Innocence Project, National Institute of Justice, and American Bar Association, and adopted in at least twenty-five states.[67]

Procedural changes to improve lineup reliability are needed because indeed, eyewitness mistakes lead to wrongful convictions. In fact, eyewitness misidentifications are widely considered to be a leading cause of wrongful convictions.[68] According

---

[58] *Id.*

[59] *Id.*

[60] *Id.* at 269.

[61] *Id.* at 274.

[62] *Id.* at 269.

[63] Steven E. Clark et al., *Regularities in Eyewitness Identification*, 32 L. & HUM. BEHAV. 187, 192 (2008) (test subjects erroneously selected a foil 21.2% of the time, correctly selected the "suspect" 46.1% of the time and made no identification 32.7% of the time).

[64] *Id.*

[65] Wells, *supra* note 48, at 277–78.

[66] *Id.* at 270–71.

[67] *Eyewitness Identification Reform*, *supra* note 21.

[68] Wells, *supra* note 48, at 259 ("Mistaken eyewitness identification is a primary cause of the conviction of innocent people.").

to the Innocence Project, 69% of DNA exonerations—252 out of 367 cases—have involved eyewitness misidentification.[69] And these exonerations represent only a small fraction of the total wrongful convictions out there that are founded on mistaken eyewitness identifications; tragically, a much larger number are, in the words of Wells, "undiscovered and undiscoverable."[70]

Even though eyewitness identifications are known to be rife with errors, they remain widespread and heavily relied upon in the criminal legal process.[71]

C. Understanding How Face Recognition Technology Is Used in Conjunction with Eyewitness Identification

As mentioned above, automated face recognition is not yet used in court as direct evidence of identity.[72] Indeed, it is likely that automated face recognition analysis would not be admissible as evidence of identity.[73] Instead, after developing a lead from face recognition technology, law enforcement representatives generally seek to have an eyewitness confirm the identification, then use the eyewitness identification as probable cause to make an arrest, and ultimately rely on the eyewitness to prosecute the arrestee.[74] When or before eyewitnesses are asked to make an identification, police sometimes tell them that face recognition technology has been or will be used to attempt to find the perpetrator.[75]

---

[69] *How Eyewitness Misidentification Can Send Innocent People to Prison*, THE INNOCENCE PROJECT (Apr. 15, 2020) [hereinafter *Eyewitness Misidentification*], https://innocenceproject.org/how-eyewitness-misidentification-can-send-innocent-people-to-prison/ [https://perma.cc/ZY7F-Q546].

[70] Wells, *supra* note 48, at 262 (explaining that exoneration by DNA testing is not an option for most people who are convicted of crimes, because few crimes other than some sexual assault crimes leave behind DNA-rich evidence that could provide definitive exculpatory evidence, and even when biological evidence exists, often it is not properly collected, preserved, and maintained.).

[71] *Id.* at 276–77.

[72] *See supra* notes 40–42 and accompanying text.

[73] *See* People v. Collins, 15 N.Y.S.3d 564, 576 (N.Y. Sup. Ct. 2015) ("The products of . . . facial recognition technology similarly can sometimes have value, but evidence produced . . . is not generally accepted as reliable by the relevant scientific communities and so cannot be admitted in trials."); People v. Reyes, 133 N.Y.S.3d 433, 436–37 (N.Y. Sup. Ct. 2020) ("There is no agreement in a relevant community of technological experts that matches are sufficiently reliable to be used in court as identification evidence.").

[74] *See supra* notes 40–42 and accompanying text; Clare Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations* (unpublished manuscript) (on file with author) ("Most, if not all agencies in the United States consider a face recognition 'possible match' to be an investigative lead only—not strong enough evidence to make an arrest.").

[75] Jackson, *supra* note 11, at 22. Jackson explains that in one client's case, "a police officer collecting surveillance told an eyewitness that he planned to run the video through [face recognition software]. A few days later the officer held a single photo identification with the civilian." *Id.*

Eyewitness confirmation may come from a showup-type procedure, in which a law enforcement representative presents only the single investigative lead to the eyewitness and asks them for a yes or no identification of that person.[76] In one case, NYPD officers used face recognition technology to generate a lead, then texted a witness a photograph of the possible match, asking, "is this the guy[?]" The witness responded, "that's the guy," and NYPD then arrested the suspect based on the eyewitness identification.[77] Researchers at the Center on Privacy & Technology report knowledge of a case in Washington, D.C. in which identification was made in a similar manner.[78]

In other cases, eyewitness confirmation is developed through a lineup (either live or as a photo array). Indeed, this seems to be a common way that law enforcement agencies across the country have used face recognition technology for over a decade. As far back as 2008, police in Philadelphia used face recognition to develop a lead based on a photograph recovered from a house where a search warrant was executed, then photographed their lead and presented him to a witness within a photo array, then arrested their suspect based on the eyewitness identification.[79] In 2013, NYPD used face recognition to develop a lead in a shooting case, then presented the suspect to witnesses in a photo array for identification and ultimately arrested the suspect.[80] In 2014, Chicago police used face recognition to develop a lead in a vehicular hijacking case, then arrested their suspect after the victim identified him from a photo array.[81] A similar process was employed by police in Palm Beach, Florida, in 2016;[82] by police in Philadelphia in 2016;[83] and by police in Chicago in 2017.[84]

---

[76] *See* NAT'L RSCH. COUNCIL, *supra* note 38, at 27–30.

[77] *Facial Recognition Motion (Redacted)*, NAT'L ASS'N OF CRIM. DEF. LAWS. (Nov. 13, 2019), https://www.nacdl.org/Document/Facial-Recognition-Motion [https://perma.cc/5M3U-RW7L]; *see* Mike Hayes, *'Is This The Guy?'*, THE APPEAL (Aug. 20, 2019), https://theappeal.org/is-this-the-guy/ [https://perma.cc/EKL4-XNLH].

[78] *See* Garvie, *supra* note 74.

[79] Brief for the Appellant, Commonwealth v. Tucker, No. 1841 EDA 2013, 2014 WL 10936613, at *5 (Pa. Super. Ct. 2014).

[80] Greg B. Smith, *Behind the Smoking Guns: Inside NYPD's 21st Century Arsenal*, N.Y. DAILY NEWS (Aug. 20, 2014), https://perma.cc/U6RJ-TH7S. This process was also employed by NYPD in its investigation of a 2013 robbery. People v. Jones, 102 N.Y.S.3d 265 (2019).

[81] Erin Meyer, *Secret Photo Taken by Cellphone App Leads Police to Carjacker: Prosecutors*, DNAINFO (Sept. 15, 2014), https://www.dnainfo.com/chicago/20140915/grand-crossing/secret-photo-taken-by-cellphone-app-leads-cops-alleged-carjacker/ [https://perma.cc/7NEL-Y4K5].

[82] Hannah Winston, *Woman ID'd by Facial-Recognition Software Arrested for Fraud*, PALM BEACH POST (Nov. 24, 2016), https://perma.cc/DW9Q-2F7Q.

[83] Alex Rose, *Yeadon Gunman Pleads Guilty to Weapons Violation*, DEL. CNTY. DAILY TIMES (Sept. 20, 2016, 8:21 PM), https://www.delcotimes.com/news/yeadon-gunman-pleads-guilty-to-weapons-violation/article_4646de13-f411-5284-a6cb-cd1238d3d05c.html [https://perma.cc/YKM2-TLQV].

[84] Tony Briscoe, *Fernwood Man Held Without Bail in Lakeview Carjacking, Sexual Assault*, CHI. TRIB. (Mar. 19, 2017, 6:08 PM), https://www.chicagotribune.com/news/break

In the recent cases of known mistaken identification involving Michael Oliver and Robert Williams, similar patterns were used. In both cases, Detroit Detective Donald Bussa used face recognition to develop a lead, then presented that person's photo to a witness as part of a photo array for identification.[85] After the eyewitness selected the photo out of the photo array, Detroit police prepared an arrest warrant and arrested the suspect based on the eyewitness identification.[86]

When presenting identification evidence at trial, prosecutors typically omit any information at all about whether and how automated face recognition technology was used during the investigation.[87] As legal scholar Megan Graham recently put it,

> [A]s things are currently playing out in cases, the prosecutors say "Well, we're not introducing the facial recognition match as evidence. What we're doing is introducing the eyewitness identification that is based on a photo array that was developed with use of facial recognition software. So in fact, we don't have to tell you that facial recognition was ever a part of this case.[88]

Instead of affirmatively disclosing information about face recognition, prosecutors have actively avoided courtroom exposure of face recognition procedures. In at least two cases, when defendants filed motions challenging law enforcement's reliance on face recognition, the prosecution simply dropped the case or offered a reduced plea deal to settle the case.[89] Thus although face recognition is used in criminal investigations frequently,[90] its use seldom has been directly scrutinized by courts.[91]

---

ing/ct-man-charged-in-lakeview-carjacking-assault-20170319-story.html [https://perma.cc/2RA6-58CT].

[85] *Oliver* Complaint, *supra* note 4, at 4; *Williams* Complaint, *supra* note 6, at 3–5 (In Mr. Williams's case, the witness was not even a person who had been present when the crime was committed, but merely someone who had viewed a surveillance video of the incident after the fact.).

[86] *Oliver* Complaint, *supra* note 4, at 4–5; *Williams* Complaint, *supra* note 6, at 2–3.

[87] *See* Garvie, *supra* note 74; Jackson, *supra* note 11, at 14.

[88] Megan Graham, Esquire, U.C. Berkeley, Panelist at the Denver Law Symposium: A.I. & Criminal Justice 21 (Feb. 12, 2021) (transcript available at https://static1.squarespace.com/static/5cb79f7efd6793296c0eb738/t/6047b6a8e3905e0d9d95bcae/1615312553120/Transcript_Crim_AI.pdf) [https://perma.cc/2T8D-27G5].

[89] *See* Mike Hayes, *'Is This The Guy?'*, THE APPEAL (Aug. 20, 2019), https://theappeal.org/is-this-the-guy/ [https://perma.cc/5M3Q-PYGJ] (stating that face recognition arguments in one case were never resolved because on the day the trial was set to begin, "prosecutors decided to significantly reduce the charges against [the defendant] from a felony to a misdemeanor with a sentence of time served"); Garvie, *supra* note 74, at 4.

[90] For example, as of August 26, 2017, the NYPD Facial Identification Section had already used face recognition technology to find possible matches over 4,000 times. *Facial Identification Section Possible Matches as of 8/26/2017*, NYPD REAL TIME CRIME CTR. (on file with Center on Privacy & Technology at Georgetown Law Center).

[91] In all three cases of Nijeer Parks, Michael Oliver, and Robert Williams, the prosecution

II. AUTOMATED FACE RECOGNITION AS A POSSIBLE DRIVER OF WRONGFUL CONVICTIONS

The central thesis of this Article is that the increased use of face recognition technology by law enforcement agencies could lead to an increase in erroneous eyewitness identifications and thus also to an increase in wrongful convictions premised on misidentifications. Face recognition technology could contribute to wrongful convictions in at least four ways: first, by generating lookalike false leads; second, by increasing the incidence of lineups in which the perpetrator is absent; third, by contributing to the creation of biased lineups; and fourth, by displacing other police technologies that could be less prone to error.[92]

A. Facilitating Generation of Lookalike False Leads

The primary reason that face recognition technology could lead to an increase in wrongful convictions is that its use sometimes will generate false investigative leads—people who are innocent but who nevertheless physically resemble the true target.

Automated face recognition applications used by law enforcement are designed to find multiple lookalikes rather than a single positive match. As discussed above, these systems purposefully escalate numerous—in some cases, hundreds of—non-matches for human consideration when queried with a probe photo of an unknown suspect, even if there is no true match for the suspect in the database.[93] If the person in a probe photo has doppelgängers in a face recognition database, these systems are designed to find them.[94]

Unrelated people can sometimes resemble each other extremely closely. Anyone who has mistaken lookalike actors for one another can attest to this.

---

dropped the charges before going to trial. *Supra* notes 1–8 and accompanying text. The use of face recognition in criminal investigation has only been directly considered by courts in a few other cases. In Lynch v. State, 260 So. 3d 1166, 1169–70 (Fla. Dist. Ct. App. 2018), a Florida appeals court considered and rejected a *Brady* argument regarding a face recognition candidate list that was not disclosed to the defendant. In People v. Knight, 130 N.Y.S.3d 919 (N.Y. Sup. Ct. 2020), a New York trial court held that the prosecution complied with discovery law when it disclosed a partial candidate list to the defense, and that disclosure of the remaining candidates was not required either under state discovery law or under *Brady*. And in People v. Reyes, 133 N.Y.S.3d 433 (N.Y. Sup. Ct. 2020), another New York Trial court considered and rejected a pretrial motion to preclude trial testimony based on the use of face recognition software, and declined to order discovery about the software.

[92] This Article offers this thesis as a hypothesis worthy of additional exploration, with an acknowledgment that its underlying propositions are theoretical and, at this point in time, largely unproven. Additional research should be performed to test the theories advanced in this Article.

[93] *Supra* notes 33–34 and accompanying text.

[94] *Id.*; *see* Jackson, *supra* note 11, at 17 ("If the software is working correctly, the suspect picked by the program should look very much like the true perpetrator . . . ."); Goldberg, *supra* note 11, at 274 ("[F]acial recognition programs are *specifically designed* to produce results that look like the perpetrator.").

Screen actor lookalikes Leighton Meester (left) and Minka Kelly (right).[95]

Actress lookalikes Margot Robbie (left) and Jaime Pressly (right).[96]

[95] "Actress Minka Kelly in 2011" by Airman 1st Class Cody Ramirez, U.S. Air Force, is a work of a U.S. Air Force Airman or employee, as part of that person's official duties. As a work of the U.S. federal government, this image is in the public domain in the United States; "Leighton Meester 2" by David Shankbone is licensed under the CC BY 2.0 license available here: https://creativecommons.org/licenses/by/2.0/deed.en.

[96] "SYDNEY, AUSTRALIA—JANUARY 23 Margot Robbie arrives at the Australian Premiere of 'I, Tonya' on January 23, 2018 in Sydney, Australia (28074883999) (cropped 3)" by Eva Rinaldi is licensed under the CC BY-SA 2.0 license available at: https://creativecommons.org/licenses/by-sa/2.0/; "Jaime Pressly at Slim-Fast Fashion Show 5" by Luke Ford is

Photographer François Brunelle amassed dozens of photographs of unrelated doppelgängers in his project titled "I'm Not a Look-Alike!"[97] including unrelated doppelgängers Charles Chason (left) and Michael Malone (right).[98]

Not only will candidate lists include lookalikes if they exist in a face recognition database, but it is inevitable that law enforcement representatives will sometimes erroneously select a lookalike as a possible match.[99] If a law enforcement representative

licensed under the CC BY-SA 2.5 license available at: https://creativecommons.org/licenses/by-sa/2.5/deed.en.

[97] François Brunelle, *I'm Not a Look-Alike!*, FRANÇOIS BRUNELLE, http://www.francoisbrunelle.com/webn/e-project.html [https://perma.cc/Q8XE-Q36P] (last visited Dec. 13, 2021); *Bio*, FRANÇOIS BRUNELLE, http://www.francoisbrunelle.com/webn/e-bio.html [https://perma.cc/NYH3-WWT5] (last visited Dec. 13, 2021).

[98] "Charles Chason and Michael Malone" by François Brunelle is licensed for use in this Article and printed with permission from the artist and subjects.

[99] This is presumably what happened in the multiple cases in which police using face recognition software have erroneously pursued the wrong person after selecting them from a candidate list.

reviews a two hundred candidate list in search of a single suspect,[100] the candidate list will contain at least one hundred ninety-nine individuals who are not the suspect but whom the system calculates to resemble the suspect more closely than other people. The person performing the analysis is bound to pick the wrong one sometimes.

This is supported by research conducted by a team of psychologists in Australia, led by David White, who simulated and studied the task of selecting a match from among a candidate list.[101] Study participants included untrained university students, facial review professionals whose job was to assess the eligibility of passport applications, and specialized facial examiners who were trained to scrutinize and compare facial images in cases of suspected fraud.[102] In numerous trials, the researchers presented a participant with a photograph of a target individual alongside photographs of eight candidates selected by face recognition software (sometimes including the target and sometimes not).[103] The participant was then instructed to decide whether the target was present in the candidate list and, if so, to select the matching candidate.[104]

The results of the White et al., study showed "very poor face matching performance in a realistic photo-to-photo matching task based on the output of commercial off-the-shelf face recognition software."[105] Notably, there was no significant performance difference between facial review professionals and untrained students.[106] When the target was present in the candidate list, these groups correctly identified the target only about 50% of the time and misidentified a lookalike about 30% of the time, and when the target was not present in the candidate list, they erroneously selected a candidate about 45% of the time.[107]

The specially trained facial examiners performed substantially better on the task, correctly identifying the target nearly 70% of the time in target-present trials and correctly determining that the target was not present about 70% of the time in target-absent trials.[108] But even the trained facial examiners incorrectly selected the wrong person approximately 10% of the time in target-present trials and approximately 30% of the time in target-absent trials.[109]

---

[100] This is the number of candidates on the candidate list generated by NYPD's system. *See supra* note 34 and accompanying text.

[101] *See* David White et al., *Error Rates in Users of Automatic Face Recognition Software*, 10 PLOS ONE 1, 10 (2015).

[102] *Id.*

[103] *Id.* at 5.

[104] *Id.*

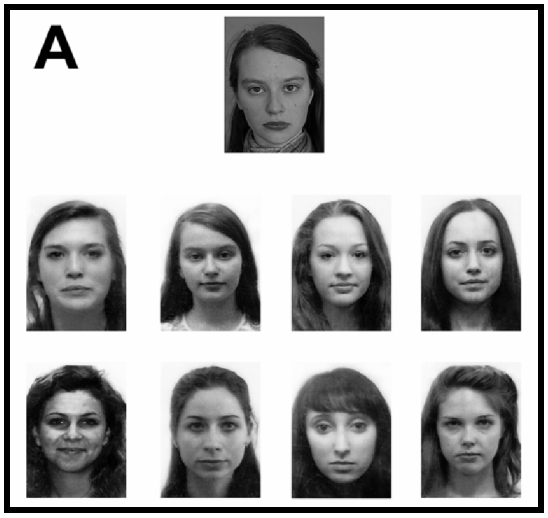
[105] *Id.* at 10.

[106] *Id.* at 8.

[107] *Id.* at 9–11.

[108] *Id.* at 8–9.

[109] *Id.* at 8.



An example of the type of simulated candidate list given to participants in the White et al. study of face recognition software users' ability to pick out matches from candidate lists.[110]

Police departments using face recognition technology agree that erroneous matches occur. In fact, James Craig, the chief of the Detroit Police Department (the department responsible for the wrongful arrests of both Michael Oliver and Robert Williams) recently stated, "If we were just to use the technology by itself, to identify someone, I would say 96[%] of the time it would misidentify."[111] A slide deck used by the Chicago Police Department to discuss face recognition technology explains, "some people look alike" and "your own interpretations can be wrong."[112] The presentation includes several side-by-side photo comparisons of unrelated people who closely resemble one another to illustrate the existence of lookalikes, cautioning users, "A high number score of a gallery image is NOT probable cause to arrest nor is the fact that a potential suspect strikingly resembles your probe image."[113]

But although departments are aware of the threat of lookalike misidentifications, mistakes do happen in real cases, as proven by the stories of Nijeer Parks, Michael Oliver, and Robert Williams.[114] In these three cases, law enforcement users of face

---

[110] *Id.* at 10. Image licensed under CC BY 3.0 U.S. license available here: https://creativecommons.org/licenses/by/3.0/us/.

[111] Jason Koebler, *Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time*, VICE (June 29, 2020, 12:56 PM), https://www.vice.com/en/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time [https://perma.cc/9WWX-BGH3].

[112] *Bureau of Detectives Presents: Facial Recognition*, CHI. POLICE DEP'T (on file with Center on Privacy & Technology at Georgetown University Law Center).

[113] *Id.*

[114] *See generally Parks* Complaint, *supra* note 1; *Oliver* Complaint, *supra* note 4; *Williams* Complaint, *supra* note 6.

recognition software developed a false lead using face recognition software—a lead that they then pursued, secured an eyewitness identification of, and ultimately arrested. NYPD similarly acknowledges that in some cases, analysts in its Facial Identification Section who were using the system misidentified the individuals they were seeking to find.[115]

Systems used by law enforcement agencies almost certainly will continue to yield false leads in the future, even as face recognition technology improves and grows more reliable over time. One reason for this is that many systems used by law enforcement agencies rely on databases of mugshot photographs that may be years or even decades old.[116] Faces change over time, and an interval of years between enrollment and search greatly reduces the ability of automated face recognition systems to recognize a face.[117] As researchers at the National Institute of Standards and Technology (NIST) have observed, "A large source of error in long-run applications where subjects are not re-enrolled is ageing."[118]

In addition, law enforcement representatives often are searching for matches to images that are not well suited for face recognition searching, such as low quality still shots captured from grainy surveillance videos or shots in which the subject's face is not turned directly toward the camera.[119] For example, according to a complaint filed by Robert Williams against the city of Detroit regarding his wrongful arrest, the surveillance camera image searched by Detroit police was a "low-resolution image" in which the perpetrator's face was "barely visible, poorly illuminated, oriented away from the camera, and partially obscured by his hat."[120]

B. Enabling User Behavior that Increases Likelihood of False Leads

In addition, human users may contribute to misidentifications by using face recognition systems in ways that further diminish the reliability of investigative leads. Research by the Center on Privacy & Technology recently revealed that law enforcement representatives frequently edit the photos they are searching, sometimes replacing features of a photographed perpetrator's face with features of entirely different people's faces that were copied and pasted from photographs found online.[121] NYPD users have even used a completely different face to conduct a search and develop an investigative lead; on at least two documented occasions, NYPD representatives

---

[115] *See Facial Identification Section Submission Summary Report*, NYPD REAL TIME CRIME CTR. (on file with Center on Privacy & Technology at Georgetown Law Center).

[116] PATRICK GROTHER ET AL., FACE RECOGNITION VENDOR TEST, NISTIR 8217 DRAFT SUPPLEMENT, NAT'L INST. STANDARDS & TECH. (2021) at 9.

[117] *Id.* at 6.

[118] *Id.* (As photographs in a face recognition reference database age, the likelihood of a probe matching with a false match grows).

[119] *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, FLAWEDFACEDATA (2019), https://www.flawedfacedata.com/ [https://perma.cc/3T3J-DRK2].

[120] *Williams* Complaint, *supra* note 6, at 19.

[121] *See* Garvie, *supra* note 74.

found they were unable to identify a suspect based on a low-quality photo, so instead simply picked celebrities that they thought looked like what they could see of the suspect's face, then developed leads based on candidate lists generated from those celebrities' faces.[122] In some cases, law enforcement representatives may have even developed leads from searches of composite sketches, which are known to be generally inaccurate.[123]

The fact that human analysts have been documented using face recognition systems in ways that may increase the likelihood of misidentification is not surprising, because there are no universal standards dictating the amount of training that human analysts must receive in order to use law enforcement face recognition systems. Agencies' face recognition policies sometimes require training, but tend to be vague on the requisite standard.[124] The Facial Identification Scientific Working Group recommends minimum training criteria for face recognition analysts that are specific and extensive,[125] but counts only five U.S. states and eight U.S. counties and cities among its members.[126] Some agencies' policies do not appear to require any training at all, such as Detroit's policy at the time when Robert Williams was being investigated.[127] And many agencies' policies are not available to the public, so their user training requirements (or lack thereof) are unknown.[128]

Indeed, analysts using face recognition software are sometimes demonstrably under-trained in how the software works or in facial comparison. For example, in one case involving face recognition, an analyst working for the Jacksonville Sheriff's

---

[122] *Id.*; NYPD, *Facial Identification*, *supra* note 31 (describing searches using the faces of actor Woody Harrelson and basketball player J.R. Smith to attempt to identify suspects who resembled them).

[123] *Id.*

[124] For example, NYPD's policy says that "NYPD personnel utilizing facial recognition technology receive training on facial recognition technology, image comparison principles, the proper operation of the technology and associated equipment." NYPD, FACIAL RECOGNITION: IMPACT AND USE POLICY 10 (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/facial-recognition-nypd-impact-and-use-policy_4.9.21_final.pdf [https://perma.cc/JPU3-BHX2]. Orlando's policy says that "Training will be provided to all authorized users of facial recognition software/technology" and "will cover both the use of facial recognition software/technology and a specific review and acknowledgment of all elements of this policy." Orlando Police Department, Policy and Procedure. 1147.1, Facial Recognition 5 (Mar. 19, 2021), https://www.orlando.gov/files/sharedassets/public/documents/opd/policies-and-procedures/police-operations/1147.1-facial-recognition.pdf [https://perma.cc/L5XM-DK8U].

[125] *See* FACIAL IDENTIFICATION SCI. WORKING GRP., MINIMUM TRAINING CRITERIA FOR ASSESSORS USING FACIAL RECOGNITION SYSTEMS (2020), https://fiswg.org/fiswg_min_training_criteria_for_assessors_using_fr_systems_v1.0_20200717.pdf [https://perma.cc/K633-V67C].

[126] *Members*, FACIAL IDENTIFICATION SCI. WORKING GRP., https://fiswg.org/members.html [https://perma.cc/L4NW-AQ6Y] (last visited Dec. 13, 2021).

[127] *Williams* Complaint, *supra* note 6, at 197.

[128] The Center on Privacy & Technology stated in 2016 that of fifty-two agencies, only four had a publicly available use policy. GARVIE ET AL., *supra* note 13, at 4.

Office seemed not to fully understand how the software works.[129] She stated in a deposition that the software "does give you a star underneath the photo if it feels that it's more likely than the other photos," and "does arrange the photos based on likeliness," but when asked what was the greatest number of stars that a candidate could receive, she said she did not know.[130]

Lookalike false leads also are likely to be unequally distributed across demographic categories, with misidentifications occurring more frequently among people of certain races and/or genders. Indeed, a growing body of research indicates that automated face recognition and other types of face analysis algorithms frequently perform unevenly across demographic groups, and that racial bias in particular has been a persistent problem, with face recognition algorithms frequently performing less well on faces of color.[131] In recent tests, some face recognition algorithms have demonstrated the ability to perform well across racial groups.[132]

Even if the software performed perfectly equally across demographic groups, the problem of lookalike false leads would still affect people of color disproportionately. One reason for this is that law enforcement agencies often exercise their authority disproportionately in communities of color.[133] In addition, many agencies' face recognition applications rely on mugshot databases containing more faces of color.[134] This leads to a somewhat higher likelihood that for any given person of color, a lookalike exists in the face recognition database.[135]

---

[129] Transcript of Deposition at 10:17–11:19, Florida v. Lynch, No. 16-2016-CF-000019, 2017 WL 11567537 (Fla. Cir. Ct. Apr. 18, 2017).

[130] *Id.* at 10:23–25.

[131] *See, e.g.*, PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, NAT'L INST. STANDARDS & TECH., FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 6 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf [https://perma.cc/7LQG-4455] (finding "empirical evidence for the existence of demographic differentials in the majority of contemporary face recognition algorithms . . . evaluated"); Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 1 (2018); Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU BLOG (July 26, 2018, 8:00 AM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [https://perma.cc/Z9D2-XUZ7].

[132] GROTHER ET AL., *supra* note 131, at 8 ("[S]ome developers supplied identification algorithms for which false positive differentials are undetectable.").

[133] Laura M. Moy, *A Taxonomy of Police Technology's Racial Inequity Problems*, 2021 U. ILL. L. REV. 139, 171–72 (2021) ("When the harmful effects of police technologies . . . are layered on top of racially discriminatory policing . . . , the result is an exacerbation of inequitable policing harms falling on black neighborhoods."); *see* THE SENTENCING PROJECT, REPORT OF THE SENTENCING PROJECT TO THE UNITED NATIONS SPECIAL RAPPORTEUR ON CONTEMPORARY FORMS OF RACISM, RACIAL DISCRIMINATION, XENOPHOBIA, AND RELATED INTOLERANCE: REGARDING RACIAL DISPARITIES IN THE UNITED STATES CRIMINAL JUSTICE SYSTEM 2–6 (2018), https://www.sentencingproject.org/wp-content/uploads/2018/04/UN-Report-on-Racial-Disparities.pdf.

[134] GARVIE ET AL., *supra* note 13, at 3, 13.

[135] *See* John J. Howard, Yevgeniy B. Sirotin, Jerry L. Tipton & Arun R. Vemury, U.S. DEP'T

Furthermore, humans tend to be unevenly skilled at identifying faces, with a general tendency to be less able to identify faces of racial groups other than the identifier's own.[136] Layered on top of potential racial bias in face recognition software and the way in which it is used, this human cross-racial identification gap is likely to compound the problem—a predominantly white police force, for example, may be even more likely to develop lookalike false leads in cases involving non-white suspects. Indeed, it is noteworthy that Nijeer Parks, Michael Oliver, and Robert Williams all are black men.[137]

C. Confusing Eyewitnesses

Rather than complementing and strengthening eyewitness identification, law enforcement use of face recognition technology may increase eyewitness confusion and error. First, because face recognition technology is likely to sometimes generate lookalike false leads, it may increase incidence of the "absence of the culprit" problem with eyewitness identifications, when a showup or lineup simply does not include the culprit.[138] Culprit-absent lineups contribute to eyewitness misidentifications because even when told explicitly that the culprit may not be in the lineup, eyewitnesses generally are not good at recognizing that the culprit is indeed absent.[139] According to one review of ninety-four experiments involving lineup simulations, when the target individual was not present in the lineup, eyewitnesses still selected someone out of the lineup 47.9% of the time.[140]

OF HOMELAND SEC., QUANTIFYING THE EXTENT TO WHICH RACE AND GENDER FEATURES DETERMINE IDENTITY IN COMMERCIAL FACE RECOGNITION ALGORITHMS (2021) (demonstrating that commercial face recognition algorithms "tended to assign higher similarity scores to different people that were the same race and/or gender.").

[136] *See* John P. Rutledge, *They All Look Alike: The Inaccuracy of Cross-Racial Identifications*, 28 AM. J. CRIM. L. 207, 211–14 (2001).

[137] Problems associated with police technologies and/or procedures, such as those discussed in this Article, also are likely to have a disproportionate impact on communities of color because police themselves have a disproportionate impact on communities of color. I have previously explained that police technology may aggravate existing racial inequity in five ways. It may (1) replicate inequity in policing, (2) mask inequity in policing, (3) transfer inequity from elsewhere to policing, (4) exacerbate inequitable policing harms, and/or (5) compromise oversight of inequity in policing. Laura M. Moy, *A Taxonomy of Police Technology's Racial Inequity Problems*, 2021 U. ILL. L. REV. 139, 143 (2021); *see also* Vincent M. Southerland, *The Intersection of Race and Algorithmic Tools in the Criminal Legal System*, 80 MD. L. REV. 487, 502–04, 507–08 (2021) .2021) (discussing how overpolicing communities of color creates biased crime data that is input into predictive algorithms. The algorithms result in false positives that create a "pernicious feedback loop" that justifies even more overpolicing).

[138] Wells, *supra* note 48, at 267.

[139] *Id.*

[140] Clark et al., *supra* note 63, at 203.

When law enforcement use of face recognition yields a false lead who resembles the true perpetrator, eyewitnesses are likely to be tricked into erroneously identifying the lead in a showup or lineup because the lead looks like the perpetrator. Research by a team of three scholars in Canada named Yarmey is illuminating.[141] The Yarmey team exposed witnesses in-person to a target individual for approximately fifteen seconds. They then asked the witnesses to pick the target out of a showup or photo lineup at different time intervals: immediately afterwards, thirty minutes later, two hours later, or twenty-four hours later. They found that when a showup was conducted two or twenty-four hours after the initial incident and a lookalike individual was shown instead of the target, witnesses falsely identified the lookalike more than 50% of the time.[142] Similarly, in a target-absent photo lineup conducted sequentially (with photos shown to the witness one at a time, rather than all at once), witnesses falsely identified the lookalike 14–33% of the time, and correctly concluded that the target was not in the lineup only 28–38% of the time.[143]

Layering the results of this study on top of those of the White et al., study helps illustrate how the use of face recognition can lead to misidentifications. Consider a scenario involving a law enforcement user as trained in facial examination as the best-performing group in the White et al., group.[144] If the user searched for a perpetrator who was captured on surveillance camera and the match did not appear in the candidate list, the White et al., study indicates that the user might nevertheless erroneously select another candidate as an investigative lead as much as 30% of the time.[145] If the user then asked an eyewitness to identify the candidate in a showup type procedure conducted just a few hours later—such as when an investigator texted a photograph to a witness and simply asked, "is this the guy?"—the Yarmey study suggests that there is a greater than 50% chance the witness would erroneously say yes.[146] Factoring these together, there could be as much as a 15% chance that when a perpetrator is not present or otherwise not found in a face recognition database used by law enforcement, a lookalike would be misidentified by law enforcement and then again by an eyewitness.[147] The actual likelihood of misidentification is unknowable because operational conditions and police procedures generally differ from the conditions applicable in these experiments, and vary widely across the law enforcement agencies. But it is easy to understand how errors both by face recognition

---

[141] *See generally* Daniel Yarmey et al., *Accuracy of Eyewitness Identifications in Showups and Lineups*, 20 L. & HUM. BEHAV. 459 (1996).

[142] *Id.* at 464. When the showup was conducted immediately, the false identification rate was 18%; at thirty minutes, the rate was 44%; at two hours, it was 58%, and at twenty-four hours, it was 53%. *Id.*

[143] *Id.* When the lineup was conducted immediately, the false identification rate was 16%; at thirty minutes, the rate was 33%; at two hours, it was 14%; and at twenty-four hours, it was 14%.

[144] *See generally* White et al., *supra* note 101.

[145] *Id.* at 2.

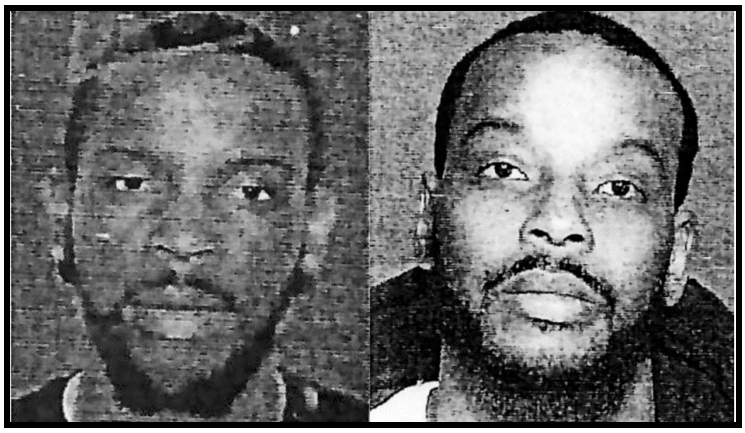
[146] *See* Yarmey et al., *supra* note 141, at 464.

[147] *See id.*

users and eyewitnesses can coincide, resulting in eyewitness-backed cases against lookalike suspects.

The fact that eyewitnesses sometimes are told that face recognition technology was used before they were asked to make an identification, as defense attorney Kaitlin Jackson has reported,[148] may further increase eyewitnesses' susceptibility to lookalikes. Because people often trust computer systems as infallible, an eyewitness who knows that automated face recognition was used to try to find the culprit may interpret this information to mean that any identification procedure in which the eyewitness subsequently is asked to participate is likely to include the culprit.[149] And research has shown that telling eyewitnesses that the culprit may be present in a lineup increases both eyewitnesses' tendency to select a lineup participant—even when the target is not present—and eyewitnesses' confidence in their selection.[150]

In the cases of Nijeer Parks and Michael Oliver, police investigators and eyewitnesses confused the men's faces with those of perpetrators in the crimes they were investigating.[151]



Man involved in Woodbridge, New Jersey incident (left) and Nijeer Parks (right).[152]

---

[148] *See supra* note 75 and accompanying text.

[149] The tendency to trust automated systems is known as "automation bias." *See* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1272 (2008) ("Automation bias effectively turns a computer program's suggested answer into a trusted final decision.").

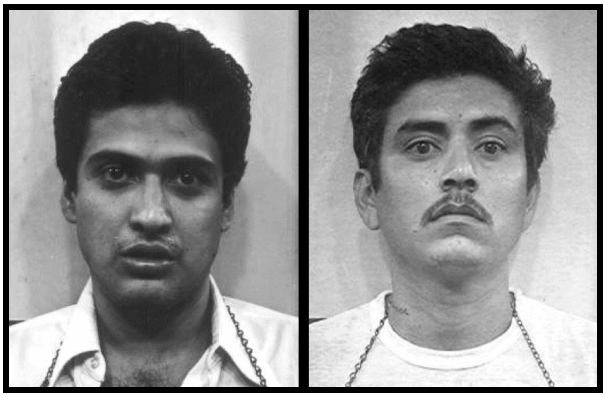
[150] Wells et al., *supra* note 39, at 21.

[151] John General & Jon Sarlin, *A False Facial Recognition Match Sent This Innocent Black Man to Jail*, CNN (Apr. 29, 2021, 12:23 PM), https://www.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html [https://perma.cc/ZWB9-3C8R]; Elisha Anderson, *Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit*, DETROIT FREE PRESS (July 10, 2020, 11:42 AM), https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/ [https://perma.cc/5T9C-Q98D].

[152] Photograph of Woodbridge, New Jersey man and Nijeer Parks by the Woodbridge Police Department is in the public domain.

Man involved in Detroit cellphone robbery (left) and Michael Oliver (right).[153]

Even without the use of face recognition technology, eyewitnesses have often been confused by faces that share some features with sought-after culprits, leading to the wrong people being prosecuted and convicted for crimes they did not commit. A recent documentary, "The Phantom," follows the case of Carlos DeLuna, who was convicted of murder—likely wrongfully—and, in 1989, executed for the crime.[154] Mr. DeLuna was identified by eyewitnesses as the murderer, but at trial, he insisted that an acquaintance of his, Carlos Hernandez, had actually committed the crime.



Carlos DeLuna (left) and Carlos Hernandez (right).[155]

[153] Photograph of man involved in Detroit cellphone robbery and Michael Oliver published in Anderson, *supra* note 151, obtained from video handout given to the press.

[154] Ben Kenigsberg, *'The Phantom' Review: The Death Penalty for a Doppelgänger*, N.Y. TIMES (July 1, 2021), https://www.nytimes.com/2021/07/01/movies/the-phantom-review.html [https://perma.cc/4WPM-NKVR].

[155] Photographs of Carlos DeLuna and Carlos Hernandez originally published in Justin Chan,

Mr. DeLuna died maintaining his innocence.[156] After his execution, an investigation spearheaded by scholar Jim Liebman and a team at Columbia Law discovered that Mr. Hernandez was a real person and brought to light strong evidence that Mr. DeLuna's claims of mistaken identity were credible.[157]

More recently, in 2017, a Kansas judge threw out the conviction of Richard Jones and released him from prison after evidence came to light that the crime may well have been committed by a different man, Ricky Amos.[158] Mr. Jones had been selected from a lineup by people who witnessed a robbery, but when those witnesses were shown photographs of Mr. Jones alongside Mr. Amos, they said they could not tell the two men apart.[159]

Richard A. Jones (left) and Ricky Amos (right).[160]

'The Phantom': The Unjust Execution of Carlos DeLuna, THE INNOCENCE PROJECT (June 11, 2021), https://innocenceproject.org/the-phantom-the-killing-of-an-innocent-man/ [https://perma.cc/6M77-YDTP].

[156] *Id.*

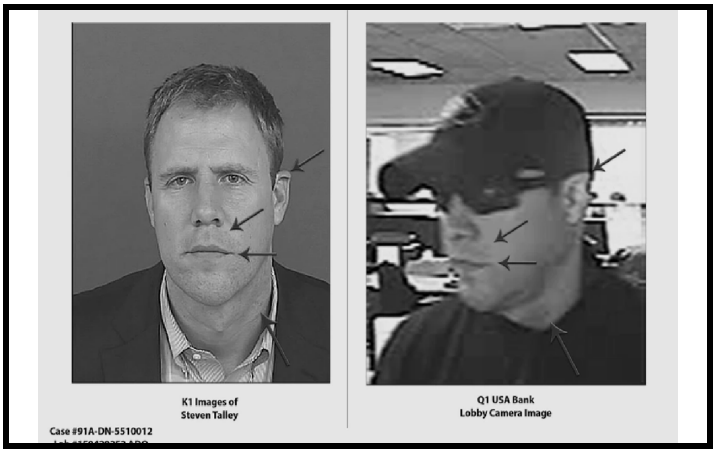
[157] *Id.*

[158] Christine Hauser, *Man Who Wrongfully Spent 17 Years in Prison in 'Doppelgänger Case' Seeks $1.1 Million*, N.Y. TIMES (Aug. 30, 2018), https://www.nytimes.com/2018/08/30/us/kansas-doppelganger-richard-jones.html [https://perma.cc/TZ89-5HC6].

[159] *Id.*

[160] Photograph of Richard A. Jones and Ricky Amos by the Kansas Department of Corrections is in the public domain and was originally published in Christine Hauser, *Man Who Wrongfully Spent 17 Years in Prison in 'Doppelgänger Case' Seeks $1.1 Million*, N.Y. TIMES (Aug. 30, 2018), https://www.nytimes.com/2018/08/30/us/kansas-doppelganger-richard-jones.html.

In yet another case, Steven Talley of Denver, Colorado, was arrested for a series of bank robberies that took place in 2014 and 2015.[161] Anonymous tipsters gave police Mr. Talley's name in response to widely circulated surveillance camera images, his estranged ex-wife agreed that it was Mr. Talley in the surveillance images, and a forensic analysis unit at the FBI compared his face to the images and concluded they were the same person.[162] Police arrested Mr. Talley violently, and he was badly injured, suffering a broken sternum, several broken teeth, four ruptured disks, blood clots in his right leg, nerve damage in his right ankle, and a possible fractured penis.[163] It later became clear that Mr. Talley was at work during one of the bank robberies and picking up food from a food bank during another, and was taller than the man who had been captured on surveillance video robbing banks.[164] The charges against him were eventually dropped, but not before he lost his job and his home.[165]



Steven Talley (left) and Denver bank robber (right).[166]

In addition, as mentioned above, in hundreds of cases in which people convicted of crimes have later been exonerated by DNA analysis, eyewitness misidentification

---

[161] Kirk Mitchell, *Man Sues FBI and Denver Police for $10 Million Claiming False Arrest for 2 Bank Robberies and Excessive Force*, DENVER POST (Sept. 15, 2016, 11:44 PM), https://www.denverpost.com/2016/09/15/fbi-denver-police-sued-false-arrest-excessive-force [https://perma.cc/7NXL-V7L7].

[162] *Id.*

[163] *See* Ava Koffman, *Losing Face: How a Facial Mismatch Can Ruin Your Life*, THE INTERCEPT (Oct. 13, 2016), https://theintercept.com/2016/10/13/how-a-facial-recognition-mismatch-can-ruin-your-life/ [https://perma.cc/FP4H-CNYN].

[164] *Id.*

[165] *Id.*

[166] Photograph of Steven Talley and Denver bank robber by the Federal Bureau of Investigation and Department of Justice is in the public domain. Photograph originally published in Koffman, *supra* note 163.

has played a central role.[167] Lookalikes played a part in some, if not many, of those cases.[168] Consider, for example, the case of John Willis, who spent more than eight years in prison for two sexual assaults before DNA analysis exonerated him and implicated another man, Dennis McGruder.[169] Mr. Willis had been arrested based on an anonymous tip after distributing a composite sketch of the perpetrator.[170] Two separate sexual assault victims and nine other eyewitnesses had all identified Willis in photo lineups.[171] Upon his exoneration, defense attorneys for Mr. Willis acknowledged that he and Mr. McGruder so closely resembled one another that witnesses easily could have mistaken one for the other.[172]

Eyewitnesses often are confused by innocent lookalikes who share some physical traits with the perpetrator. That problem is likely to intensify in instances where face recognition software has been used, increasing the likelihood that a suspect will, at the very least, be someone who closely resembles the perpetrator.

D. Displacing Traditional Techniques

The foregoing problems are, of course, only problems specific to face recognition technology if the use of face recognition technology results in meaningful differences relative to the status quo. In other words, if lookalike false leads and misidentifications are just as likely to occur without the use of automated face recognition technology, then there is no cause for particular concern about the introduction and use of this new technology.

One reason the adoption of face recognition technology may increase lookalike false leads relative to the status quo is that over time, greater reliance on automated face recognition to generate leads may displace traditional techniques that are less prone to the generation of lookalike false leads. For example, neighborhood canvassing—going door-to-door in an area and painstakingly interviewing everyone who might have seen or otherwise know something relevant—is an important early step in traditional crime-solving.[173] But if investigators find that they can more quickly and efficiently

---

[167] *Eyewitness Misidentification*, *supra* note 69.

[168] THE INNOCENCE PROJECT, 200 EXONERATED: TOO MANY WRONGFULLY CONVICTED 18–19 (2016), https://www.innocenceproject.org/wp-content/uploads/2016/10/ip_200.pdf [https://perma.cc/WWE2-4BVU] (summarizing the wrongful convictions of two hundred people, 77% of which were to some degree based on misidentification).

[169] Maurice Possley, *Prisoner to Go Free as DNA Clears Him in Beauty Shop Rape*, CHI. TRIB. (Feb. 24, 1999), https://www.chicagotribune.com/news/ct-xpm-1999-02-24-9902240103-story.html [https://perma.cc/PH9R-PYF5].

[170] James R. Acker, *The Flipside Injustice of Wrongful Convictions: When the Guilty Go Free*, 76 ALBANY L. REV. 1629, 1673–74 (2013).

[171] THE JUST. PROJECT, EYEWITNESS IDENTIFICATION: A POLICY REVIEW 12, https://web.williams.edu/Psychology/Faculty/Kassin/files/Justice%20Project%20-%20on%20ET.pdf [https://perma.cc/72CC-9ABY].

[172] Possley, *supra* note 169.

[173] *See* Ramesh Nyberg, *Going Door to Door*, POLICE MAG. (July 1, 2006), https://www

identify a lead by capturing a still shot from a nearby surveillance camera and running it through a face recognition database, traditional canvassing may fall by the wayside or not be conducted as thoroughly. Indeed, the Security Industry Association has promoted face recognition technology to law enforcement as an improvement on "traditional methods" such as canvassing areas with photos.[174] Writing for *Security* magazine, Eric Hess of SAFR from RealNetworks (a face recognition vendor) suggests that face recognition software can help law enforcement identify potential suspects when agencies cannot spare the resources necessary to canvass an area on foot.[175]

Events in the real cases against Nijeer Parks, Michael Oliver, and Robert Williams illustrate how reliance on face recognition technology may displace or overshadow traditional investigatory techniques.[176] In the case against Nijeer Parks, investigators did not engage in the most basic detective work to link Mr. Parks to the scene of the crime. When Mr. Parks self-reported to police to clear up the mistake, no one even investigated his alibi (he was at a pharmacy in Haledon, New Jersey, when the incident happened), which turned out to be provable.[177] Nor did the investigators secure any supporting evidence to place him at the scene of the crime, such as fingerprints in the rental car that the perpetrator drove into a parked car and abandoned in a nearby parking lot.[178] Investigators also ignored the fact that the perpetrator appeared to wear earrings, but Mr. Parks does not have his ears pierced.[179] In the case against Robert Williams, the Detroit Police Department did not even attempt to solve the crime for over five months.[180] According to the complaint Mr. Williams filed against the department, when an investigator finally did begin to look into the case, he "[r]esort[ed] to facial recognition technology as his first method of investigation."[181] In the case against Michael Oliver, police ignored the fact that Mr. Oliver has tattoos up and down both arms and the perpetrator did not, and arrested Mr. Oliver anyway.[182]

Even if face recognition technology is only relied upon by law enforcement in circumstances when traditional methods have been tried and have failed to yield a

---

.policemag.com/339574/going-door-to-door [https://perma.cc/S2RD-NFBT] ("The area canvass—knocking on the doors of all the residences surrounding the crime scene—is one of the first tasks a lead detective should have on his lead sheet.").

[174] Jake Parker, *Facial Recognition Success Stories Showcase Positive Use Cases of the Technology*, SEC. INDUS. ASS'N (July 16, 2020), https://www.securityindustry.org/2020/07/16/facial-recognition-success-stories-showcase-positive-use-cases-of-the-technology/ [https://perma.cc/7UDX-BUYW].

[175] Eric Hess, *Top Five Misconceptions About Face Recognition*, SEC. MAG. (Apr. 28, 2020), https://www.securitymagazine.com/articles/92242-top-five-misconceptions-about-face-recognition [https://perma.cc/KC7B-PP7W].

[176] *See* Hill, *supra* note 3.

[177] *Parks* Complaint, *supra* note 1, at 3–5; *see* Hill, *supra* note 3.

[178] *Parks* Complaint, *supra* note 1, at 4.

[179] *See* General & Sarlin, *supra* note 151.

[180] *Williams* Complaint, *supra* note 6, at 18.

[181] *Id.*

[182] Anderson, *supra* note 151.

viable lead, its use could lead to an increase in the total number of cases solved, with some unknown portion of the solved cases simply being cases of misidentification.

E. Evading Challenges

Whatever the impact of face recognition technology on rates of misidentification and wrongful conviction is, current practices will make it difficult to evaluate in real cases.[183] As mentioned briefly above, face recognition matches are not yet used as direct evidence of identity in court; instead, law enforcement typically relies only on eyewitness identification, and often does not even disclose the fact that face recognition was used to develop an investigative lead in the first place.[184] This deprives judges and juries of the opportunity to assess whether and how eyewitness identification reliability might be affected when face recognition technology was used to generate the initial investigative lead. Defendants also are not given the chance to challenge face recognition technology when its use is not disclosed in court.

Defendants also are not able to explore either the existence of lookalikes or the possibility that a different lookalike actually committed the crime. Exploring these possibilities would require defendants to be given a copy of the candidate list from which their photo was selected, but those candidate lists are virtually never disclosed. Some have argued that candidate lists should be disclosed under *Brady v. Maryland*.[185] Few courts have considered this question, but so far none have required disclosure of a candidate list under *Brady*.[186] In limited circumstances, some of the secrecy may be lifting—in one recent case, the prosecution disclosed some information regarding face recognition technology in an effort to comply with state discovery law.[187]

Faced with persuasive eyewitness testimony against them, even innocent defendants sometimes will simply plead guilty in exchange for reduced charges and sentences, further limiting opportunities to shed light on misidentifications fostered by face recognition technology. Nijeer Parks considered pleading guilty to a reduced charge and even discussed the possibility with his family, even though he was innocent, because he had previous felony convictions and would have received a long sentence if he were convicted of another felony.[188] He told *60 Minutes*, "I knew I didn't do it, but it's like, I got a chance to be home, spending more time with my son, or I got a chance to come home, and he's a grown man and might have his own son."[189]

---

[183] *How Accurate Is Facial Recognition Today?*, REC FACES (Nov. 5, 2020), https://recfaces.com/articles/how-accurate-is-facial-recognition [https://perma.cc/5VHG-UQAN].

[184] *Supra* notes 97–100 and accompanying text.

[185] *See generally* Brady v. Maryland, 373 U.S. 83 (1963); *see* Jackson, *supra* note 11, at 20–21; Goldberg, *supra* note 11, at 276–88.

[186] *See infra* note 221.

[187] *Id.*

[188] Hill, *supra* note 3.

[189] Anderson Cooper, *Police Departments Adopting Facial Recognition Tech Amid*

III. RECOMMENDATIONS

Policymakers must act swiftly to address the role that face recognition technology already plays in misidentifications and possible wrongful convictions. As a result of this widespread technology, there is a near certainty that others in addition to Nijeer Parks, Michael Oliver, and Robert Williams have been misidentified and wrongfully arrested or even prosecuted and convicted.

Policymakers should consider rejecting the use of face recognition technology by law enforcement altogether, in light of its likely role facilitating lookalike misidentifications.[190] Face recognition technology is excellent at finding people who closely resemble one another, and humans—even when they are well trained—are not able to tell the difference between true matches and lookalikes consistently and reliably.[191] As a result, misidentifications may simply be an unavoidable outcome of law enforcement use of face recognition technology. Worse, the extent to which this technology coupled with eyewitness identification may be driving misidentifications and wrongful convictions—a potentially tremendous harm—has not been measured, thus making it impossible to perform an informed analysis regarding how big the problem is and what should be done about it.

Allegations of Wrongful Arrests, CBS NEWS (May 16, 2021), https://www.cbsnews.com/news/facial-recognition-60-minutes-2021-05-16/ [https://perma.cc/4TR2-48WM].

[190] A number of others have suggested that the best way to protect against various harms caused by face recognition technology would be to ban it altogether. *See generally, e.g.*, Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOYOLA L. REV. 101 (2019); Evan Selinger & Woodrow Hartzog, *The Case for Banning Law Enforcement from Using Facial Recognition Technology*, THE JUST. COLLABORATIVE INST. (Aug. 2020), https://30glxtj0jh81xn8rx26pr5af-wpengine.netdna-ssl.com/wp-content/uploads/2020/12/20.08_Facial-Recognition-1.pdf [https://perma.cc/YS9Q-S77Q]; Lindsey Barrett, *Ban Facial Recognition Technologies for Children—and for Everyone Else*, 26 B.U. J. SCI. & TECH. L. 223 (2020); Evan Greer, *Don't Regulate Facial Recognition. Ban it.*, BUZZFEED NEWS (July 18, 2019), https://www.buzzfeednews.com/article/evangreer/don't-regulate-facial-recognition-ban-it [https://perma.cc/ZSK3-SCRQ]; Luke Stark, *Facial Recognition is the Plutonium of AI*, 25 XRDS 50 (2019); Jennifer Lynch, *Clearview AI—Yet Another Example of Why We Need a Ban on Law Enforcement Use of Face Recognition Now*, ELEC. FRONTIER FOUND. (Jan. 31, 2020), https://www.eff.org/deeplinks/2020/01/clearview-ai-yet-another-example-why-we-need-ban-law-enforcement-use-face [https://perma.cc/L53S-WFEW]. And, indeed, some jurisdictions have already banned face recognition. *See* Kate Conger, Richard Fausset & Serge F. Kovaleski, *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html [https://perma.cc/9EN5-PGUE]; Rachel Metz, *Beyond San Francisco, More Cities Are Saying No to Facial Recognition*, CNN (July 17, 2019), https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html [https://perma.cc/JEK6-7QS3]; David Gutman, *King County Council Bans Use of Facial Recognition Technology by Sheriff's Office, Other Agencies*, SEATTLE TIMES (June 1, 2021), https://www.seattletimes.com/seattle-news/politics/king-county-council-bans-use-of-facial-recognition-technology-by-sheriffs-office-other-agencies/ [https://perma.cc/JF77-YG28].

[191] *See* discussion *supra* notes 152–55 and accompanying text.

Going even further, policymakers should also consider, more fundamentally, whether a criminal prosecution should *ever* be able to rest on eyewitness identification alone, when the suspect is not someone that the eyewitness already knows. One way to frame the current research regarding humans and computers performing face recognition tasks is to say that humans are not able to identify faces consistently and reliably, even with the assistance of powerful face recognition software that, according to at least one leading expert, performs this task "better than humans."[192] As Justice Frankfurter once said, "[t]he identification of strangers is proverbially untrustworthy."[193] If eyewitness identification cannot be trusted, then it should not be relied upon. In the words of scholar Sandra Guerra Thompson, "in the absence of other extrinsic evidence linking the suspect to the crime . . . the legal system is simply incapable of confirming the accuracy of an eyewitness's identification."[194]

Given the fundamental unreliability of eyewitness identification, policymakers should adopt a rule requiring corroborating evidence in cases involving eyewitness identification, as Thompson has recommended.[195] As justification for such a rule, she points out, "[a]s a simple matter of known probabilities, the scientific literature makes a compelling case that a single eyewitness's identification of a stranger, especially under the typical circumstances present in serious crimes, does not constitute proof 'beyond a reasonable doubt.'"[196] Therefore, Thompson calls for the legislature or the judiciary to preclude convictions based solely on eyewitness identification, except when the victim knows the culprit through a relationship that predates the crime.[197] Cases involving stranger identification would thus require "genuine investigative work to uncover other independent evidence linking the suspect to the crime."[198]

If policymakers are to permit law enforcement to use automated face recognition as an investigative tool, then at a minimum, the corroboration requirement that Thompson recommends must apply to eyewitness identifications of leads developed with the use of face recognition software. Without such a corroboration requirement, there is simply too great a risk that lookalike false leads will be misidentified and pursued, subjected to great disruption and distress, wrongfully deprived of their freedom, convicted, and imprisoned.[199] If the only evidence against an individual suspected of committing a crime is an eyewitness identification by a stranger, law enforcement agencies should be compelled to go gather more evidence before they can make an arrest.

---

[192] Cooper, *supra* note 189.

[193] Felix Frankfurter, *The Case of Sacco and Vanzetti*, THE ATLANTIC (Mar. 1927), https://www.theatlantic.com/magazine/archive/1927/03/the-case-of-sacco-and-vanzetti/306625/.

[194] Sandra Guerra Thompson, *Beyond a Reasonable Doubt? Reconsidering Uncorroborated Eyewitness Identification Testimony*, 41 U.C. DAVIS L. REV. 1487, 1506 (2008).

[195] *See generally id.*

[196] *Id.* at 1524.

[197] *Id.* at 1541.

[198] *Id.* at 1542.

[199] *Supra* Part II.

In addition, rules should be established requiring prosecutors to disclose to defendants any information about use of face recognition technology during an investigation, along with the details needed to evaluate the reliability of the resulting potential match, including the image that was searched (the "probe" photo) and the candidate list with confidence scores and photos of other candidates. The candidate list arguably constitutes *Brady* material that could serve to exculpate a defendant in the event that they were wrongfully selected from a candidate list that also included the true perpetrator.[200] This question has not yet been thoroughly addressed by courts,[201] but policymakers need not wait for the courts—they can simply decide that candidates have a right to know when face recognition technology was used in their case, and that candidate lists have important exculpatory value and therefore should be disclosed. For an idea of how to do this, policymakers should look to New York State, which now requires prosecutors to proactively disclose certain information to defendants that previously was not disclosed by default.[202]

Many policy reforms that address face recognition technology specifically have been recommended by others and may well be needed, but because this Article focuses on the interaction between face recognition technology and eyewitness identification, the recommendations detailed here are driven by that interaction and the resultant implications for eyewitness identification policy. Policymakers must adopt reforms to eyewitness identification procedures to minimize misidentifications and ensure that the proper procedures are followed and enforced. Policymakers should consider prohibiting showups, which are inherently suggestive, or at the very least should prohibit photographic showups and strictly limit the circumstances under which in-person showups may be used.[203]

---

[200] *See* Jackson, *supra* note 11, at 20–21; Goldberg, *supra* note 11, at 276–88.

[201] There are two exceptions that I am aware of. The first is in the case of Willie Lynch, a Florida defendant who, after he was convicted, appealed in part on the grounds that under Brady v. Maryland, 373 U.S. 83 (1963), he should have had access to the full list and photos of candidates returned by the face recognition software, on the belief that lookalike candidates would have cast doubt on the case against him. The court rejected the argument, reasoning that Lynch had failed to show there was a reasonable probability that disclosure of the candidate list would have changed the outcome of the trial. Lynch v. State, 260 So. 3d 1166, 1169–70 (Fla. Dist. Ct. App. 2018); s*ee* Goldberg, *supra* note 11, at 278–79. The second is the case of Casey Knight, in which a New York trial court held that the prosecution complied with discovery law when it disclosed a partial candidate list to the defense, and that disclosure of the remaining candidates was not required either under state discovery law or under *Brady*. People v. Knight, 130 N.Y.S.3d 919 (N.Y. Sup. Ct. 2020).

[202] CTR. FOR COURT INNOVATION, DISCOVERY REFORM IN NEW YORK: SUMMARY OF MAJOR LEGISLATIVE PROVISIONS 1 (2019).

[203] *See* Wells et al., *supra* note 39, at 7. On the issue of photographic showups, Wells et al. states, "it should be apparent that there should never be such a thing as a photographic showup. . . . [T]here is no reasonable excuse for not taking the time to embed the photo among filler photos and conduct a proper photo lineup." *Id.*

Policymakers also should adopt policies requiring widely recognized practices demonstrated to reduce the likelihood of misidentification and supported by The Innocence Project, National Institute of Justice, American Bar Association, and International Association of Chiefs of Police, among others:

- A "double-blind" lineup, in which the person responsible for setting up the lineup differs from the one who administers it, so that neither the administrator nor the eyewitness knows who the suspect is;
- Instructions given to the eyewitness that are designed to deter the eyewitness from feeling compelled to make a selection, including the statement that the culprit may not be present in the lineup;
- Efforts made when composing the lineup to ensure that the suspect does not match the eyewitness's initial description of the perpetrator more closely than the fillers, and generally does not stand out from the fillers in any way;
- Collection of a "confidence statement" from an eyewitness immediately following the lineup procedure, articulating the level of confidence the eyewitness has in their identification of a suspect; and
- Thorough documentation of the lineup procedure—ideally, electronic recording.[204]

The Innocence Project reports that twenty-five states have implemented these core reforms either through legislation, court action, or substantial voluntary compliance.[205] State policymakers increasingly are receptive to identification procedure reforms in light of mounting evidence that such reforms truly reduce the risk of wrongful convictions.[206]

Two items on this list of best practices warrant additional considerations in jurisdictions where police are permitted to use face recognition technology. First, regarding eyewitness instructions, it is important not only that the instructions state that the culprit may not be present in the lineup, but also that police do not tell eyewitnesses when they have employed automated face recognition to try to find the culprit.[207] This is because, as discussed above, disclosing the use of face recognition technology to eyewitnesses may increase misidentifications.[208] Second, regarding

---

[204] *Eyewitness Identification Reform*, *supra* note 21; IACP L. ENF'T POL'Y CTR., EYEWITNESS IDENTIFICATION (2016), https://dps.mn.gov/divisions/bca/bca-divisions/investigations/Documents/IACP-Eyewitness-Identification-policy.pdf [https://perma.cc/DDW8-2YTF]; Wells et al., *supra* note 39, at 7.

[205] *Eyewitness Identification Reform*, *supra* note 21.

[206] *See* Michael Ollove, *Police Are Changing Lineups to Avoid False IDs*, PEW CHARITABLE TR. (July 13, 2018), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2018/07/13/police-are-changing-lineups-to-avoid-false-ids [https://perma.cc/KD2Q-RBLT].

[207] At present, police sometimes disclose to eyewitnesses that they will use or have used automated face recognition to try to develop a lead. *Supra* note 76 and accompanying text.

[208] *See* discussion *supra* notes 149–50 and accompanying text. Wells et al., *supra* note 39,

fillers in a lineup, when automated face recognition has been used to develop a lead who, if they are not the actual perpetrator, closely resembles the perpetrator, the best fillers to minimize the likelihood of lookalike misidentification may be other people who are also very close in appearance to the perpetrator. This is because research suggests that when an innocent lookalike is presented as a suspect in a lineup, they are more likely to be misidentified by an eyewitness if the fillers are dissimilar from them in appearance.[209]

In the absence of strong policies and careful oversight, police often do not follow eyewitness identification best practices, including in cases in which their investigative lead was developed with the existence of face recognition technology. In all three of the misidentifications of Nijeer Parks, Michael Oliver, and Robert Williams, police failed to adhere to the above-enumerated practices. In the cases of Michael Oliver and Robert Williams, police conducted a photo lineup, but allegedly did not do so in a double-blind manner.[210] In the case against Nijeer Parks, it seems likely that no lineup was conducted at all.[211] And as discussed above, police in multiple jurisdictions have been known to use highly suggestive showup procedures to positively identify suspects after using face recognition technology to develop their lead.[212]

In light of the increasing use of automated face recognition as an investigative tool, policymakers should hasten the adoption of the above-enumerated widely supported reforms to identification procedures.[213] In addition, advocates should consider updating their materials to explain how the increasing use of face recognition

---

at 21. As a result, Wells et al. argue, "when inviting an eyewitness to attend a lineup procedure, police should not suggest that a suspect has been arrested or that the culprit will be present in the identification procedure." *Id.*

[209] *See* Melissa F. Colloff, Brent M. Wilson, Travis M. Seale-Carlisle & John T. Wixted, *Optimizing the Selection of Fillers in Police Lineups*, PROC. NAT'L ACAD. SCIS. U.S.A., Feb 23, 2021, at 4 ("[W]hen the innocent suspect happens to be similar to the perpetrator (an innocent lookalike), the use of low-similarity fillers should increase the false-alarm rate."). Having conducted a series of experiments to test eyewitness performance on lineup tasks, the researchers generally conclude that it is best to select fillers who are *dissimilar* to the suspect. *Id.* But they note that this approach is likely to increase the misidentification rate in instances where the suspect is an innocent lookalike of the perpetrator. *Id.* When face recognition technology has been used to develop a lead, every suspect is likely to be a lookalike of the perpetrator.

[210] *Oliver* Complaint, *supra* note 4, at 4; *Williams* Complaint, *supra* note 6, at 4–5.

[211] *See* General & Sarlin, *supra* note 151. It is unclear whether investigators in Mr. Parks's case even conducted a photographic showup with an eyewitness. Two eyewitnesses reportedly confirmed to police that the photo on a fake ID left at the scene of the crime was a photo of the suspect, and the police then issued a warrant for Mr. Parks's arrest based on a face recognition match with that photo. *Id.*

[212] *Supra* notes 84–86 and accompanying text.

[213] Rebecca Darin Goldberg has also written about how face recognition underscores the need for identification procedure reforms. Goldberg, *supra* note 11, at 292–93.

technology supports the urgent need to improve reliability of eyewitness identifications. The most broadly circulated materials advocating for these reforms currently make no mention of the use of face recognition technology.[214]

Policymakers should also adopt additional reforms suggested by a subcommittee of the Executive Committee of the American Psychology-Law Society, led by eyewitness identification expert Gary Wells, which was tasked with updating scientific guidelines for eyewitness identification procedures.[215] The subcommittee released a paper detailing its findings and recommendations in 2020.[216]

In particular, policymakers should adopt the subcommittee's recommendation on evidence-based suspicion: that an individual should never be included in an identification procedure unless there are evidence-based grounds to suspect that they are guilty of the specific crime being investigated, and that that evidence should be documented in writing prior to including the suspect in an identification procedure.[217] Wells et al. explain in their report that this recommendation "derives from the observation that there are no laws or other mechanisms in place to prevent jurisdictions from making investigative decisions that result in extremely low base rates for culprit-present lineups (i.e., a high rate of culprit-absent lineups)."[218] As discussed above and as illustrated in the cases of Nijeer Parks, Michael Oliver, and Robert Williams, the use of face recognition technology could, without an evidence-based suspicion requirement, facilitate the construction of culprit-absent lineups.[219] An evidence-based suspicion requirement would help reduce the risk that lookalikes will be investigated and pursued by law enforcement for crimes they did not commit, based on their physical appearance alone, to their great inconvenience or even harm.

CONCLUSION

Face recognition technology is often embraced by policymakers as a tool that can make law enforcement investigations more efficient and successful. But this technology comes with serious risks, including the possibility that its use increases the incidence of misidentifications and wrongful convictions. Policymakers should swiftly step in and adopt policy changes that are urgently needed to mitigate the risk of misidentifications.

---

214 *See Eyewitness Identification Reform*, *supra* note 21.
215 Wells et al., *supra* note 39.
216 *Id.*
217 *Id.* at 11–14.
218 *Id.* at 11.
219 *See* discussion *supra* Section II.C.