LINCOLN MEMORIAL UNIVERSITY
LAW REVIEW

VOLUME 10 FALL 2022 ISSUE 1

MAN VS. MACHINE: FACIAL RECOGNITION TECHNOLOGY REPLACING EYEWITNESS IDENTIFICATIONS

Stefanie M. Bowen[1]

I. INTRODUCTION

A video uploaded to Facebook, titled "Peacefully storming the Capital (sic)" on January 10, 2021, shows many individuals pushing their way into the U.S. Capitol building days earlier.[2] The individual filming the video panned the camera from the doorway to the crowd pushing from behind, revealing the U.S. Supreme Court and the Library of Congress in the background.[3] An alarm sound echoes over the video as the individual holding the camera turns the lens on his face.[4] The man addresses the camera: "In the Capitol baby, yeah!"[5] Broken glass is visible on the ground, and individuals are pouring out the doors to escape the U.S. Capitol as the man

[1] Stefanie M. Bowen, Juris Doctor, May 2022, LMU Duncan School of Law.
[2] Criminal Compl. at 11, United States v. Mark Simon, 2021 U.S. Dist. Court Pleadings 400, (D.D.C. Feb. 2, 2021) (1:21-cr-00067-ABJ).
[3] *Id.* at 13.
[4] *Id.*
[5] *Id.* at 15.

pushes further into the building.[6] The camera pans back to his face again as he shouts, "2021 Donald Trump!"[7]

On January 16, 2021, the Federal Bureau of Investigation ("FBI") submitted the above-mentioned video to the Operations Technology Division ("OTD") for further review.[8] An OTD representative informed the FBI in Los Angeles that a biometric search of driver's license photos revealed the identity of the man filming the January 6 insurrection uploaded to Facebook.[9] The computer algorithm, confirmed by a trained forensic investigator, identified the man in the video as Mark Simon of Huntington Beach, California.[10] On January 21, 2021, two weeks after the Capitol riots, a criminal complaint filed against Mark Simon accused him of violating Title 18 U.S.C. § 1752(a)(1) and (2), Entering or Remaining in Restricted Buildings or Grounds; and Title 40 U.S.C. § 5104(e)(2)(D) and (G), Unlawful Activities on Capitol Grounds and Disorderly Conduct.[11] An investigation that, years prior, would have been nearly impossible led to a criminal complaint in just two weeks.[12]

The January 6, 2021, riots at the U.S. Capitol shocked the minds and hearts of those who respect the democratic process. Understandably, the lowest point in American democracy ushered in a sense of urgency to identify the perpetrators. Since January 6, 2021, the FBI, in tandem with other law enforcement agencies at the federal, state, and local levels, has worked tirelessly to identify those who illegally entered the Capitol building, damaged property, and, in some cases, injured or killed Capitol officers. Technology, especially facial recognition

---

[6] *Id.* at 14.
[7] *Id.* at 15.
[8] *Id.* at 18.
[9] *Id.*
[10] *Id.*
[11] *Id.* at 3.
[12] Drew Harwell & Craig Timberg, *How America's Surveillance Networks Helped the FBI Catch the Capitol Mob*, THE WASH. POST, (Apr. 2, 2021, 9:00 AM), https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/ ("If the event happened 20 years ago, it would have been 100 times harder to identify these people," said Chuck Wexler, executive director of the Police Executive Research Forum, a D.C.-based think tank. "But today it's almost impossible not to leave your footprints somewhere.").

software, is a cornerstone of these investigations. Clearview AI, a leading facial recognition company used by law enforcement, reported a 26% uptick in use on January 7, 2021.[13]

Traditionally, police and prosecutors relied on eyewitness identification. Often a witness or a victim would provide a description of the events, identify a suspect in a line-up or show-up, or identify a suspect in court. Eyewitness identification testimony is so persuasive. It is often the most compelling testimony available at trial. Yet while it is so persuasive, it is often so inaccurate and unreliable.

Recognizing the limitations of eyewitness identification, it is tempting to believe that facial recognition technology can be an effective, safe replacement. An algorithm should, in theory, be less biased than a human. The video remembers and relates what a victim, under stress, may not. As evidenced in the January 6 investigations, facial recognition technology is quick and can give police leads when, often, leads dry up. But while many laud the efforts of law enforcement's use of facial recognition software in apprehending Capitol rioters, it is important to keep in mind the consequences of deploying and expanding the use of this emerging technology. There are concerns with facial recognition technology, especially the realities of police use of this technology against minorities. There are significant concerns that the facial recognition software's embedded bias places minorities at a disadvantage in the criminal justice system. When the dust settles from January 6, what remains is the unregulated use of technology in policing—technology with embedded biases for minorities historically targeted, disproportionately, by law enforcement. So, while in theory, a machine should outperform man, in some cases, it is no better than the eyewitness identification historically viewed as biased and inaccurate. Deploying this technology without recognizing this fact and putting significant rules in place risks public safety. What is more, without regulation of facial recognition technology use, police risk harming the public trust. A perfect storm following the Capitol storm. Can machines really replace man? Should they?

---

[13] Johana Bhuiyan, *Facial recognition may help find Capitol rioters – but it could harm many others, experts say,* LA TIMES (Feb. 4, 2021, 6:00 AM), https://www.latimes.com/business/technology/story/2021-02-04/facial-recognition-surveillance-capitol-riot-black-and-brown-communities?utm_source=pocket_mylist.

This Note addresses facial recognition algorithms as a replacement for eyewitness identifications. Part I addresses the pitfalls of traditional eyewitness identifications and the Court's efforts to mitigate those pitfalls. Part II addresses the capabilities of facial recognition software as a viable investigative tool. In particular, this section addresses facial recognition algorithms as a law enforcement investigative tool, the software's limitations, and a lack of regulation. Part III discusses the similarities and differences between eyewitness identification and facial recognition algorithms. Finally, Part IV suggests solutions to the risks inherent in facial recognition technology to strike a fair balance between law enforcement's need to use the tool and the public's need for accuracy and transparency.

II. PART I. EYEWITNESS IDENTIFICATION (AND MISIDENTIFICATION).

Eyewitness identification is a cornerstone of police investigations and criminal prosecutions.[14] Indeed, police often rely on eyewitness identifications to develop leads, narrow investigations, and establish reasonable suspicion.[15] Likewise, prosecutors rely on eyewitness identifications in court,[16] and research suggests juries are highly influenced by eyewitness testimony at trial.[17] Former Supreme Court Justice William Brennan Junior once famously said, "There is almost nothing more convincing than a live human being who takes the stand, points a finger at the defendant, and says 'That's the one!"[18]

And yet, despite the persuasive nature of eyewitness identification, in the courtroom and elsewhere, studies show

---

[14] POLICE EXECUTIVE RESEARCH FORUM, A NATIONAL SURVEY OF EYEWITNESS IDENTIFICATION PROCEDURES IN LAW ENFORCEMENT AGENCIES (2014), https://www.ojp.gov/pdffiles1/nij/grants/242617.pdf.

[15] Beth Schuster, *Police Lineups: Making Eyewitness Identifications More Reliable*, 258 NAT'L INSTIT. OF JUST. J. 2 (2007).

[16] POLICE EXECUTIVE RESEARCH FORUM, *supra* note 1 at 14.

[17] ELIZABETH LOFTUS & KATHERINE KETCHAM, WITNESS FOR THE DEFENSE: THE ACCUSED, THE EYEWITNESS, AND THE EXPERT WHO PUTS MEMORY ON TRIAL (St. Martin's Press 1991).

[18] Watkins v. Sowders, 449 U.S. 341, 352 (1981) (Brennan, J. dissenting).

that eyewitness identification is incredibly unreliable.[19] According to The Innocence Project, a nonprofit focused on exonerations and criminal justice reform, eyewitness identification is the leading cause of wrongful convictions.[20] The numbers support this statement. In 367 cases in which DNA evidence resulted in an exoneration, 252 of the convictions were based on erroneous eyewitness identifications.[21] What is more, nearly 450 more cases based on erroneous eyewitness identification resulted in exoneration without accompanying exculpatory DNA evidence.[22] The statistics show that 700 or more individuals, some with long prison sentences, faced life-altering consequences, mainly because of misidentification.[23] Misidentification, beyond the impact on the wrongfully convicted, stands to undermine public trust in the justice system and law enforcement. What, then, makes eyewitness identification so unreliable yet so persuasive?

A. EYEWITNESS IDENTIFICATION IS HISTORICALLY VALUED AND TRUSTED.

---

[19] State v. Guilbert, 306 Conn. 218, 235-36 (2012) ("The extensive and comprehensive scientific research, as reflected in hundreds of peer-reviewed studies and meta-analyses, convincingly demonstrates the fallibility of eyewitness identification testimony and pinpoints an array of variables that are most likely to lead to a mistaken identification.").

[20] *Eyewitness Identification Reform*, THE INNOCENCE PROJECT, https://innocenceproject.org/eyewitness-identification-reform/ (last visited Apr. 22, 2022) ("Mistaken eyewitness identifications contributed to approximately 69% of the more than 375 wrongful convictions in the United States overturned by post-conviction DNA evidence.").

[21] Innocence Staff, *How Eyewitness Misidentification Can Send Innocent People to Prison*, THE INNOCENCE PROJECT, (April 15, 2020), https://innocenceproject.org/how-eyewitness-misidentification-can-send-innocent-people-to-prison/.

[22] *Id.*

[23] *Id.* 252 cases of DNA exculpating a person sentenced with eyewitness testimony and 450 cases exculpating a person sentenced with eyewitness testimony not using DNA evidence totals 717 exonerees.

From religion to modern-day memoir, the first-person account of experiences has long been valued and sought. Religious texts often use first-person experience allegory to relate moral lessons.[24] The Quran, the Old Testament, the New Testament, and other ancient texts like the Hindu Smriti (Sanskrit, meaning "that which is remembered") relay the first-person experience.[25]

In more recent times, memoirs have been known to intrigue the public and often appear on best sellers' lists.[26] The memoir genre relays first-person point-of-view experiences of those in the public light or those experiencing great tragedy and triumph.[27] Television in the 21st century continues the tradition of seeking first-person accounts of experiences with "reality shows" that show experiences of the "stars" and intersperse interviews with the subjects for even more first-hand accounts.[28] And beyond the public's fascination with the story, the storytellers in memoirs and television convey the human desire to describe and record experiences from our perspective.

---

[24] Thomas D. Albright, *Why eyewitnesses fail*, 114 PROC. NAT'L ACAD. SCI. U.S. 7758, 7759 (2017), https://www.pnas.org/doi/epdf/10.1073/pnas.1706891114.

[25] *Id.*

[26] For example, *The Diary of a Young Girl*, also known as *The Diary of Anne Frank* is perhaps the best-known memoir, appearing on various best-sellers lists since its English publication in 1952. Other memoirs capturing the public fascination include Ernest Hemingway's *A Moveable Feast* and Henry David Thoreau's *Walden*. More recently, the memoirs of Michelle Obama, Dolly Parton, and even SNL actress Tina Fey have topped the list. The public embraces memoirs of all genres—politics, entertainment, and even serial killers like John Wayne Gacy, who published a memoir in 1993.

[27] Jessica Dukes, *What is a Memoir?*, CELADON BOOKS, https://celadonbooks.com/what-is-a-memoir/ ("More focused than an autobiography, a memoir is an intimate look at a moment in time.").

[28] Bradley Babendir, *Stop Feeling Embarrassed by How Much You Love Reality TV*, WASH. POST (May 14, 2018, 3:48 PM), https://www.washingtonpost.com/entertainment/books/stop-feeling-embarrassed-by-how-much-you-love-reality-tv/2018/05/14/3c550e5c-579f-11e8-8836-a4a123c359ab_story.html ("[The book by Mann] . . . probes at what memoir and reality tv share . . .").

Scientific research is another example of the human desire to understand and report firsthand observations.[29] Scientific research, especially the scientific method, is based on objective records of observation and experience.[30]

Sports also rely on the human interpretation of events. Umpires and referees in all sports are relied on to relay and interpret events and make decisions based on those experiences.[31]

Given the historical importance and interest in the recording and transmitting of firsthand experiences, it's unsurprising that individuals are often called on and indeed relied on to give testimony about an experience he or she witnessed. From ancient lore to modern sports activities, humans are interested in and rely on eyewitness stories and accounts and show a predilection to trust the experience of others. But science, as it turns out, suggests they should not.

B. SEEING ISN'T ALWAYS BELIEVING.

How someone first sees an event influences how the event is remembered and eventually relayed.[32] When two people see the same object, they may walk away with wildly different interpretations. Recall the "Blue or Gold Dress" phenomenon that swept the internet in 2015.[33] Some saw the dress as blue with black stripes, while others insisted the dress

---

[29] Albright, *supra* note 24, at 7759.

[30] *Id.*

[31] Eric S. Hintz, *The Invention of Instant Replay*, SMITHSONIAN NAT'L MUSEUM OF AM. HIST. (Jan. 20, 2022), https://invention.si.edu/invention-instant-replay (Instant replay was invented in 1963 during an Army-Navy football game. Despite initial resistance from referees, the National Football League (1986), the National Hockey League (1991), the National Basketball Association (2002), and Major League Baseball (2008) eventually adopted instant replay to aid officiating.).

[32] Albright, *supra* note 24, at 7760.

[33] Terrence McCoy, *The Inside Story of the 'White Dress, Blue Dress' Drama that Divided a Planet*, WASH. POST (Feb. 27, 2015, 1:57 AM) https://www.washingtonpost.com/news/morning-mix/wp/2015/02/27/the-inside-story-of-the-white-dress-blue-dress-drama-that-divided-a-nation/.

was gold with white stripes.[34] How could two individuals seeing the same photo come to such drastically different conclusions? While the meme led to many debates, it also illustrated how the human eye and brain operate to give each person a different perspective.[35] Much of what we perceive of color depends on lighting and perspective. A backlit photo would suggest a shadow, while a front-lit photo would suggest no shadow present.[36] Indoor and outdoor lighting also makes a difference.[37]

The human brain seeks context. The original photo of the dress was taken on a cellular phone, in poor lighting, with little background for context.[38] Given the lack of context for a human to judge the lighting conditions, whether it was plagued by shadow, or if the photo was taken indoors, each person's brain began to fill in the blanks, automatically, to make the best conclusion.[39]

This isn't a phenomenon unique to internet memes. The human brain, in all situations, seeks to contextualize and fill in the blanks. A witness may relay a memory just as it exists in his or her mind, but the memory is affected by context and the blanks the brain filled in to complete the picture in the mind's eye. So, while the memory may be relayed accurately, the memory itself may be inaccurate given the perspective of the witness or the brain's struggle to fill in context.

C. EYEWITNESS IDENTIFICATION IS A TEST OF MEMORY.

---

[34] *Id.*

[35] *Id.*

[36] Pascal Wallisch, *Two Years Later, We Finally Know Why People Saw "The Dress" Differently*, SLATE (Apr. 12, 2017, 10:48 AM) https://slate.com/technology/2017/04/heres-why-people-saw-the-dress-differently.html.

[37] *Id.*

[38] Wallisch, *supra* note 36.

[39] Melissa Hogenboom, *Why Does the Human Brain Create False Memories?*, BBC (Sept. 29, 2013) https://www.bbc.com/news/science-environment-24286258 ("Our perceptual systems aren't built to notice absolutely everything in our environment. We take in information through all our senses but there are gaps . . . [s]o when we remember an event, what our memory ultimately does is fill in those gaps by thinking about what we know about the world.").

Human memory is not a video recorder. Even acknowledging that a witness's memory may be at first imprinted on the brain with incorrect context, memory itself is fallible and deteriorates over time. Research as early as the 1800s acknowledged the fact that as time passes after an event, a memory of the event deteriorates exponentially.[40] If the ability to recall memory is 100% moments after the event, as time progresses, recall ability drops to 40% just 90 minutes after the event.[41] Two days after the event, the ability to recall is typically just 20%, and there it remains.[42] An eyewitness typically describes the event more than 90 minutes after it happens. This "forgetting curve" may impact an eyewitness's ability to recall the event before an investigation begins.[43]

Research also suggests that memory recall is not the only aspect that deteriorates as time marches on. Memories seem to literally fade. In a Boston study, people consistently remembered visual scenes as being less vibrant than they were originally experienced.[44] An eyewitness simply may be unable to recall the memory as vividly and will therefore have less detail to relay. The Boston College researchers studying this phenomenon hypothesize the dulling of memories occurs because of both passage of time (part of the forgetting curve) and interference of new information.[45] So, as time marches on, an eyewitness's ability to accurately identify a perpetrator may lessen as the memory becomes less vivid due in part to forgetting and in part to additional information they may receive.

At bottom, eyewitness identifications, in court and out of court, are a test of memory. In other words, the quantity of

---

[40] HERMANN EBBINGHAUS, MEMORY: A CONTRIBUTION TO EXPERIMENTAL PSYCHOLOGY (trans., Henry A. Ruger, Colum. Univ. N.Y. City Tchr.'s Coll. 1913), https://archive.org/details/memorycontributi00ebbiuoft/page/n5/mode/2up; *see also* Innocence Staff, *supra* note 21.

[41] Innocence Staff, *supra* note 21.

[42] *Id.*

[43] *Id.*

[44] Rose A. Cooper et al., *Memories Fade: The Relationship Between Memory Vividness and Remembered Visual Salience*, 30 J. PSYCH. SCI. 657 (2019).

[45] Ed Hayward, *Memories Persist, Details Fade*, BC NEWS (May 2019), https://tinyurl.com/memoriesfade.

memory deteriorates with the "forgetting curve," and research also suggests the quality of the memory fades with time.

D. CROSS-RACE MISIDENTIFICATION AFFECTS EVERYONE.

Eyewitness identifications are generally inaccurate for the many reasons just described. But when the factor of race is considered, they become even more inaccurate.[46] Cross-race identifications occur when the witness and the defendant being identified are of different racial backgrounds.[47] Psychologists have found two basic causes underlying the inaccuracy of cross-race identifications.[48] First, a lack of expertise with other races, and second, the tendency of the brain to categorize and label faces rather than seeing a face individually.[49] Either cause would be enough to reduce the accuracy of cross-race recognition, but together they are extremely unreliable.[50]

Individuals lack expertise with other races.[51] Expertise, in this context, refers to the experience in observation. Despite the work of many, communities in the United States tend to remain informally segregated largely.[52] This *de facto* segregation leads to more interaction with same-race faces than with faces of a race not our own ("cross-race" faces).[53] The inability to identify cross-race faces remains true for all races—those who live in predominantly white communities will interact with more white persons, while those who live in predominantly African American communities will interact with more African American persons. Continued exposure over time develops "expertise" for recognizing and identifying individual

---

[46] Taki V. Flevaris & Ellie F. Chapman, *Cross-Racial Misidentification: A Call to Action in Washington State and Beyond*, 38 SEATTLE U. L. REV. 861, 870-871 (2015).

[47] John Paul Wilson & Kurt Hugenberg, *The Cross-Race Effect and Eyewitness Identification: How to Improve Recognition and Reduce Decision Errors in Eyewitness Situations*, 7 SOC. ISSUES & POL'Y REV. 83 (2013).

[48] *Id.* at 87.

[49] *Id.* at 87-90.

[50] *Id.* at 87.

[51] *Id.*

[52] *Id.*

[53] John Paul Wilson & Kurt Hugenberg, *The Cross-Race Effect and Eyewitness Identification: How to Improve Recognition and Reduce Decision Errors in Eyewitness Situations*, 7 SOC. ISSUES & POL'Y REV. 83, 87 (2013).

features.[54] This expertise develops a greater accuracy for differentiating facial features in those same race faces to which you are disproportionately exposed.[55] In other words, individuals simply have more experience with same-race faces in a *de facto* segregated society. Exactly how the expertise permits the memory to recall and differentiate facial features is a matter of some scientific debate.

Some scientists hypothesize that exposure creates expertise that allows us to efficiently extract information—like the location of the eyes relative to the nose—in same-race faces.[56] Our brains can quickly process the features of same-race faces and recall the relationship between the features because we are consistently exposed to similar examples.[57] These scientists argue an individual's memory and recall of same-race faces is impacted by our memory.[58] By having an extensive number of same-race faces in our memory for recall, the memory is biased toward same-race faces and the ability to discriminate between them.[59] In other words, we have more images banked in our memory to recall and compare.

The second explanation for the ease of same-race identification (and thus the difficulty in cross-race identification) lies in the human brain's desire to categorize the things we see, including people.[60] It's "automatic, pervasive, and spontaneous."[61] The action of categorization begins without our awareness—a subconscious urge to contextualize what we see.[62] The human brain sees a person and begins to file the person into "folders" of age, sex, and race.[63] The categories, for our brain, allow navigation of social situations.[64] We can predict behaviors to expect and thus adjust our own behaviors.[65] But when we make these snap decisions, filing

---

[54] *Id.*
[55] *Id.* at 88.
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] *Id.* at 90.
[61] *Id.*
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.*

someone away as "black" or "biracial" or "white," we may not move past the category and determine what differentiates an individual from others like them.[66] Faces in the same category, then, blend.[67]

A risk emerges in categorization, especially in a society where we are not exposed to other races because of *de facto* segregation. Categorization paired with *de facto* segregation means our brain may see some categories as "less relevant" and thus unnecessary to continue processing.[68] For example, if you live in a *de facto*, informally racially segregated world, members of a cross-race may—sadly—seem less personally relevant.[69] If you don't have a reason to move beyond the category label, finding individual characteristics of cross-race faces becomes much less likely.[70] The brain is likely to stop at categorizing by age, sex, and race and may not move on to make the connections required for expertise.[71]

If an eyewitness has categorized a face by race but lacks the expertise that comes with both extended exposures, more examples to recall and compare in memory, and less attention to the detail of the features, the risk of misidentification is extremely high. When the risk of cross-race misidentification pairs with the other difficulties found in eyewitness identification—a human brain that fills in blanks, sometimes inaccurately, reliance on memory that is fallible, the risk of suggestive procedures used by police—reliance on the eyewitness testimony of a human becomes almost unthinkable. And yet juries continue to find eyewitness testimony to be some of the most compelling evidence available.

E. EYEWITNESS IDENTIFICATIONS CAN BE MANIPULATED, KNOWINGLY AND UNKNOWINGLY.

Beyond the limitations of eyewitness identification caused by imperfect memory and life experience, outside

---

[66] John Paul Wilson & Kurt Hugenberg, *The Cross-Race Effect and Eyewitness Identification: How to Improve Recognition and Reduce Decision Errors in Eyewitness Situations*, 7 SOC. ISSUES & POL'Y REV. 83, 90 (2013).
[67] *Id.*
[68] *Id.* at 91.
[69] *Id.*
[70] *Id.*
[71] *Id.*

forces, such as other humans, can influence eyewitness identification, both knowingly and unknowingly. Detectives and members of law enforcement may knowingly use unnecessarily suggestive tactics like placing a minority suspect in a lineup of Caucasians. On the other hand, they may unknowingly influence the process with unintentional influential body language or statements.

i. SOME TACTICS ARE OBVIOUSLY UNNECESSARILY SUGGESTIVE.

Whether a suspect is asked to appear in a live identification lineup, or his image is used in a photo array, there may be circumstances that are so unnecessarily suggestive and conducive to mistaken identification that a suspect is denied due process of law.[72] In *Wade*, the Supreme Court of the United States contemplated procedures that police historically used that were overly suggestive.[73] These tactics included: (1) placing the suspect in a lineup with "grossly dissimilar" individuals; (2) placing the suspect in a lineup before a witness who knows all of the lineup participants except the suspect; (3) placing the suspect in a lineup and making the suspect alone wear distinctive clothing that was allegedly worn by the perpetrator; (4) telling the witness that the culprit has been caught and then bringing the suspect alone before the witness or allowing the suspect to be viewed in jail; (5) placing the suspect in a lineup and pointing out the suspect to the witness before or during the lineup; (6) asking participants in the lineup to try on a piece of clothing that fits only the suspect; and (7) allowing witnesses to see the suspect in police custody before the lineup.[74] The procedures described in *Wade*, in 2022, seem alarmingly suggestive, obviously impermissible investigative conduct. Indeed, lineups conducted in this way before the Court fashioned remedies to combat such practices resulted in many misidentifications in cases and subsequent presentation of testimony in court.

---

[72] *See* Stovall v. Denno, 388 U.S. 293 (1967) (where the Court first contemplates unnecessarily suggestive line ups violate the Due Process Clause of the Fourteenth Amendment).
[73] United States v. Wade, 388 U.S. 218 (1967).
[74] *Id.* at 233.

ii. SOME POLICE TACTICS ARE UNINTENTIONALLY SUGGESTIVE.

While the tactics in *Wade* seem obviously suggestive, some tactics for eyewitness identification in police lineups are less so. For instance, one study conducted by trained psychologists staged a crime during a lecture.[75] Nearly 100 students witnessed the crime, and "police" provided two control groups with the opportunity to identify the suspect in a lineup.[76] The researchers then crafted subtle differences in the two sets of instructions provided to participants.[77] One instruction implied that the witness had to choose among the suspects in the lineup, while the other set implied that the witness did not have to make a choice.[78] The researchers then included the criminal who appeared in the classroom in the lineup only half the time.[79] The results showed that instructing the witnesses in a manner that did not suggest they must make an identification resulted in fewer misidentifications.[80] In other words, asking, "Is the suspect in the lineup?" allowed witnesses to refrain from making a choice, thus choosing a person incorrectly.[81] What is more, the instruction did not prevent the positive identification of the correct suspect when they were in the lineup.[82] At bottom, it seems that subtle differences in language used by police can have a potentially catastrophic effect on a suspect if it is suggestive.

Other research shows that police confirmation or suggestive body language or tone about the accuracy of a witness's choice can affect the identification itself and the confidence a person has in the identification.[83] Inflating the confidence of an eyewitness after selection in a lineup risks projecting that confidence onto a jury. The unreliable

---

[75] Roy S. Malpass & Patricia G. Devine, *Realism and Eyewitness Identification Research*, 4 L. & HUM. BEHAV. 350 (1981).
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.* at 350-351.
[80] *Id.* at 351.
[81] *Id.*
[82] *Id.*
[83] K.V. Erickson, *Function of Nonverbal Police Communication*, 43 POLICE CHIEF J. 48, 49 (1976).

identification, again, becomes so persuasive when presented to a jury that is prepared to accept a witness's memory as infallible.

iii. RELIABILITY IS THE MOST IMPORTANT ASPECT.

Of course, the Court has, since the late 1960s, addressed overly suggestive police lineup tactics from two angles. First, as suggested above, overly suggestive tactics involving lineups and showups alike may be challenged as violative of the minimum standards of fairness in a criminal trial.[84] These challenges are permissible even before the Sixth Amendment right to counsel attaches. Second, once in the "critical stage" of prosecution, a suspect's Sixth Amendment right to counsel attaches, and counsel must be present during lineups.[85]

To address due process concerns, in 1977, the Court announced a test in *Mason v. Brathwaite* to examine the totality of the circumstances of identifications before a decision on admissibility.[86] The Court previously recognized that tainted identifications risk violating Due Process and undermining the integrity of the judicial system in *Stovall* and *Biggers*.[87] But a rule that banned all suggestive identification scenarios was simply too narrow for the Court.[88] While there is a concern, as outlined in *Wade* and *Gilbert*, with eyewitness identifications, the police investigation tactic serves a purpose.[89] The Court in *Manson* conceded that an eyewitness may be testifying about an encounter with a total stranger, and the recollection may be influenced by the circumstances of the emergency or human emotion.[90] Furthermore, police tactics may also distort the witness's recollection.[91] Even so, a per se ban would prevent a jury from hearing reliable and relevant evidence.[92]

---

[84] Manson v. Brathwaite, 432 U.S. 98 (1976).
[85] U.S. CONST. amend. VI.
[86] *Manso*n, 432 U.S. at 112.
[87] *See generally*, Stovall v. Denno, 388 U.S. 293 (1967); Neil v. Biggers, 409 U.S. 188 (1972).
[88] United States v. Wade, 388 U.S. 218, 240 (1967).
[89] *Id.*
[90] *Manson*, 423 U.S. at 112.
[91] *Id.*
[92] *Id.* at 110.

Instead, suggestive identifications won't violate Due Process if there are "significant indicia of reliability."[93] In other words, even some unnecessarily suggestive procedures may result in admissible eyewitness identifications if there is a showing that the eyewitness identification was nonetheless reliable. The factors to consider when determining reliability were outlined in a previous case, *Neil v. Biggers*, 409 U.S. 188 (1972).[94] The factors include: (1) the opportunity of the witness to view the defendant, (2) the witness' degree of attention, (3) the accuracy of the witness's prior description of the criminal, (4) the witness' level of certainty with his identification, and (5) the time between the crime and the identification.[95]

This totality of the circumstances approach, juxtaposed with a per se ban, gives the benefit of influencing police behavior as well as the administration of justice.[96] While a per se rule might have the most significant effect on deterrence, a totality examination can also motivate law enforcement to guard against unnecessarily suggestive procedures for fear the evidence might be inadmissible.[97] The totality approach, unlike the per se approach, permits the admission of evidence that is reliable where a per se approach might deny a trier of fact the ability to examine such information.[98] The totality approach also promotes the fair administration of justice when it allows some reliable information to be viewed by a trier of fact, unlike a per se ban.[99] The Court's rule in *Manson* allows police the room to operate while also acknowledging the risk of unreliable identification.

Of course, there are best practices that law enforcement can implement, just as contemplated in *Manson* to increase the reliability of witness identifications in subtly suggestive scenarios. Because overly suggestive and unreliable lineups and photo arrays risk inadmissibility, police now have written policies to direct eyewitness identifications. The FBI and DOJ encourage these procedures. These policies serve to hold

---

[93] *Id.* at 188 (Stevens, J. concurring).
[94] *Biggers*, 409 U.S. at 199-200.
[95] *Id.* at 199.
[96] *Manson*, 432 U.S. at 112.
[97] *Id.*
[98] *Id.*
[99] *Id.*

agencies accountable to the public and to the courts and mitigate the risk of unreliable identifications. One policy involves crafting neutral lineup instructions for a witness. This mitigates the risk a witness might feel pressure to select a suspect in a lineup.[100] Giving the witness the knowledge that the suspect may or may not be present is one way to ensure neutral instructions.[101] The research presented above suggests that neutral instructions prevent misidentification and do not hinder the positive identification of the correct suspect.[102]

Additionally, the unintentional cues of police officers, like body language and tone, can be suggestive, but using "double-blind" procedures easily overcomes this suggestion.[103] The officer conducting the lineup with the witness should know nothing about the suspect in the lineup or whether the suspect is in the lineup.[104] A double-blind procedure prevents body language or tone that suggests a witness is correct or incorrect and allows the witness to freely examine the choices without monitoring an officer's reaction.[105] This can prevent inflated confidence that can be transmitted to a jury.

Even with written procedures, court rules, and a healthy understanding of the risks of eyewitness identification, the fact remains that eyewitness identifications are incredibly persuasive, but also incredibly unreliable.

F. IS THERE A BETTER WAY?

As evident in the discussion in Part I, eyewitness identification is so persuasive. Jurors, as laypersons, rely on eyewitness identification in everyday life. First-person allegories, video replay, and memoirs serve to perpetuate public reliance and emphasis on first-person eyewitness recounts. Even so, eyewitness identification is so unreliable. Eyewitness identification relies on human memory. Human memory is susceptible to the constraints of time, the pressure of an emergency, and the general limitations of the ability to recall

---

[100] OFFICE OF JUSTICE PROGRAMS, U.S. DEP'T OF JUSTICE, EYEWITNESS EVIDENCE: A GUIDE FOR LAW ENFORCEMENT REPORT 19 (1999), https://www.ojp.gov/pdffiles1/nij/178240.pdf [hereinafter, EYEWITNESS EVIDENCE].

[101] *Id.*

[102] Malpass, *supra* note 75, at 350.

[103] EYEWITNESS EVIDENCE, *supra* note 100, at 9.

[104] *Id.*

[105] *Id.*

information. Further, our experiences impact our ability to differentiate appropriately between members of other races. Additionally, police tactics, blatant or subtle, may influence an eyewitness's memory during an identification lineup. The limitations of the human memory and a witness's identification, coupled with a jury's limited information on the risks of such identifications, create an environment where Courts must try to educate a jury while also using the totality of the circumstances to conclude whether there are sufficient indicia of reliability in an eyewitness's account. Rather than relying on the fallible human memory, police procedures, or expert testimony, is there a way to eliminate the human element entirely? Can facial recognition technology that uses artificial intelligence rather than human intelligence alleviate the concerns that persist in the world of eyewitness identification?

III. PART II. FACIAL RECOGNITION TECHNOLOGY: CAN MACHINE REPLACE MAN?

Given all the difficulties that surround human eyewitness identification, such as imperfect memory, cross-race misidentification risks, and the risk of unduly suggestive tactics, it is natural to seek a solution that involves less human interaction. Algorithms are increasingly present in our daily lives; according to a 2021 study by the University of Georgia, humans may trust algorithms more than other humans when it comes to decision-making.[106] In fact, human trust in an algorithm increases as the difficulty of the task increases.[107] In other words, when faced with a tough decision, humans may prefer to have a computer "do it for them."[108]

Recognizing the complexities and difficulties present in eyewitness identification, particularly related to the limitation of human memory, it feels natural to assume an algorithm might perform the task with less error. Facial recognition technology, using an algorithm to find similar faces using varying databases, is a police investigation tool that some suggest can or should replace the need for eyewitness identification in the investigation period. As discussed in the

---

[106] Eric Bogert et al., *Humans rely more on algorithms than social influence as a task becomes more difficult*, 11 SCI. REP. 8083 (2021).
[107] *Id.*
[108] *Id.*

introduction, departments deployed facial recognition technology widely to assist in the investigation of the January 6 Capitol riots. But are there limitations? Does facial recognition technology eliminate the risk of cross-race misidentification? Can it build public trust where eyewitness identifications risk erosion?

A. HOW FACIAL RECOGNITION TECHNOLOGY WORKS.

To understand the risks and limitations of facial recognition technology, we must understand how it works. You may be intimately familiar with facial recognition technology from everyday use. Likely, your cellular phone uses biometric identification passwords—comparing a stored photo of you with a current, live image to determine whether it is the same person.[109] Law enforcement uses the same technology used in your iPhone.[110]

Essentially, facial recognition technology can take a face in a crowd from a video, like a body-worn camera video, and compare it against a database of stored images, like a state driver's license photo database. The comparison determines whether the face in the crowd matches a face in the database.[111] Facial recognition begins by finding a person's face within a photo or video.[112] This is known as face detection.[113] The face is then "normalized" by scaling, rotating, and uniformly aligning the image for comparison.[114] The technology then takes the normalized face image, measures its features, and identifies different landmarks on the face that can be quantified.[115] The

---

[109] Apple Support, *About FaceID advanced technology*, APPLE, https://support.apple.com/en-us/HT208108 (last visited Apr. 26, 2022).

[110] *Id.* Apple FaceID operates like all other facial recognition technology—by measuring points on the face and verifying whether the image placed before the camera is the same image saved previously.

[111] Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org [hereinafter, *Perpetual Lineup*].

[112] *Id.*

[113] *Id.*

[114] *Id.*

[115] *Id.*

depth of cheeks, the distance between eyes, the size of the forehead, and the texture of the skin are all translated into a numerical pattern called an algorithm.[116] The algorithm represents a "faceprint" much like a fingerprint—a unique pattern assignable to a person.[117] The algorithm takes this faceprint (also called a probe photo) and examines other photos in the database of stored images. Then, the algorithm issues a score to reflect the similarity of their features.[118]

While facial recognition technology works to compare two images to determine whether it is the same person, there is no "yes" or "no" answer.[119] Rather, facial recognition technology identifies matches as "more likely" or "less likely."[120] Most software in use by law enforcement will produce a selection of "top" photos with the most similarities or a group of photos that are rated above a certain threshold.[121] Most software uses a "star" rating.[122] The individuals in these rated photos become targets of further investigation.

B. POLICE USE FACIAL RECOGNITION TECHNOLOGY IN MANY SETTINGS.

Most facial recognition software used by law enforcement agencies is developed by private companies.[123]

---

116 *Id.*

117 U.S. GOV'T ACCOUNTABILITY OFF., GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 3 (2015), https://www.gao.gov/assets/gao-15-621.pdf. "A faceprint . . . is . . . a digital code that a facial recognition algorithm creates from an image."

118 *Id.*

119 *Perpetual Lineup*, *supra* note 111.

120 *Id.*

121 *Id.*

122 *See generally* BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES 36–45 (Joseph N. Pato & Lynette I. Millett, eds., National Academies Press 2010) (hereinafter "Pato Report").

123 Julie Horowitz, *Tech Companies are Still Helping Police Scan Your Face*, CNN BUSINESS (July 3, 2020, 8:36 AM), https://www.cnn.com/2020/07/03/tech/facial-recognition-police/index.html ("Clearview AI, Japan's NEC and Ayonix, Germany's Cognitec and Australia's Omniscient have all said they intend to maintain their relationships with US police forces . . ."). *See*

The technology, however, is not new. The first fully automated facial recognition algorithm appeared in the early 1990s.[124] Local, state, and federal police agencies use face identification functions to identify unknown faces.[125] In 2016, a study of law enforcement use of facial recognition software, the most extensive research to date, estimated more than one in four of all American state and local law enforcement agencies have the power to run face recognition searches on their databases or partner with another agency to run a search.[126] The FBI face recognition unit (FACE Services) searches at least 16 state driver's license databases.[127] The Department of Defense, Drug Enforcement Administration, Immigration and Customs Enforcement, and even the IRS and Social Security Administration have access to one or more state or local face recognition systems.[128] In fact, 2016 data showed that face recognition searches of driver's license databases at the FBI are six times more common than federal court-ordered wiretaps.[129]

Understanding that law enforcement is using this technology, it's important to know exactly how they deploy it in the field. Law enforcement agencies perform four basic tasks using facial recognition software. The tasks include stop and identify, arrest and identify, investigate and identify, and real-time video surveillance.

i. STOP AND IDENTIFY

---

also Drew Harwell, *Amazon Extends Ban on Police Use of Its Facial Recognition Technology Indefinitely*, WASH. POST (May 18, 2021, 3:32 PM), https://www.washingtonpost.com/technology/2021/05/18/amazon-facial-recognition-ban/. Amazon enacted a one-year moratorium on police use of its facial recognition technology.

[124] Matthew Turk & Alex Pentland, *Eigenfaces for Recognition*, 3 J. COGNITIVE NEUROSCI. 71, 72 (1992).

[125] *Perpetual Lineup, supra* note 111, at III.C.

[126] *Id.*

[127] *Id.*

[128] *Id.*

[129] *Id.* From 2011 to 2015, federal judges authorized 6,304 wiretaps. In that same period, FBI used FACES Services 214,920 searches.

While on patrol, an officer may briefly stop an individual for questioning.[130] If the individual has no identification or refuses to identify herself, an officer can take a photo using a smartphone or tablet and use facial recognition technology to compare the photo to other images in a database of images.[131] The database may include mug shots, driver's license photos, or images from other investigations.[132] As described above, the software will compare the facial features of the detained individual with existing photos in a database and produce "top" matches with the most similarities.[133]

ii. ARREST AND IDENTIFY

Upon arrest and during booking, arrestees are photographed for a mugshot. This mugshot is, at some departments, enrolled in a mugshot database.[134] The mugshot itself may be compared to existing mugshots in the database or may be compared to a driver's license database or unsolved crimes photo file database.[135] Some departments submit the mugshot to the FBI for inclusion in FACE Services.[136] The FBI, then, of course, runs the new photo against existing photos and catalogs the new mugshot for future searches.[137]

iii. INVESTIGATE AND IDENTIFY

Sometimes, indeed in 2022, quite often, a crime occurs in front of a camera. This might be a security camera, a smartphone in the hands of a bystander, or a social media post by the perpetrator.[138] This image, in the hands of police, may be searched against the described databases of mugshots, driver's

130 Terry v. Ohio, 392 U.S. 1 (1968) (holding a brief detention, based on reasonable suspicion, comports with the Fourth Amendment of the United States Constitution).
131 *Perpetual Lineup*, *supra* note 111, at III.C.
132 *Id.*
133 *Id.*
134 *Id.*
135 *Id.*
136 *Id.*
137 *Id.*
138 *Id.*

license photos, or unsolved photo files.[139] This is a powerful tool in developing leads, determining whether crimes are connected, or determining whether a suspect is operating under a pseudonym.[140]

iv. REAL TIME VIDEO SURVEILLANCE

Though expensive and sometimes difficult to obtain, some departments are using real-time video surveillance.[141] A series of photos gathered from various sources (mugshot databases, driver's license databases, and unsolved crime files, as previously described) comprise a "hot list" of wanted persons uploaded to a database.[142] The program extracts live video from a camera positioned at a chosen location and compares the hot list to passersby. A match results in an alert to the department.[143]

C. ALGORITHMS AND ACCURACY

Facial recognition technology is powerful. Police can and do use the tool to solve crimes and develop leads in cases. As stated above, in the case of the Capitol riots, investigations that previously might take weeks or months and endless manpower are completed quickly. However, with great reward comes great risk. An inaccurate result from a facial recognition search results in the arrest and potential conviction of the wrong person. Are the tools, then, accurate and reliable?

i. FACES IN GENERAL.

No system is 100 percent accurate under all conditions.[144] Facial recognition technology, as a tool, is less

---

[139] *Id.*
[140] *Id.*
[141] *Perpetual Lineup*, *supra* note 111, at III.C.
[142] *Id.*
[143] *Id.*
[144] Jennifer Lynch, *Face Off: Law Enforcement Use of Facial Recognition Technology* , ELECTRONIC FRONTIER FOUNDATION (Feb. 12, 2018), https://www.eff.org/wp/law-enforcement-use-face-recognition.

accurate than fingerprint identification.[145] How could this be? Fingerprints are fairly consistent over time.[146] Of course, an accident or repetitive motion can alter them, but in general, fingerprints are unique to an individual and remain so over time.[147] On the surface, faces, like fingerprints, are individual and consistent.[148] After all, we spent a significant time exploring how faces are subtly different, and humans with bias may not take the time to notice small but important differences.[149] Faces are unique, and there are subtle differences that aid recognition and recall.[150] But, faces also have a unique difference from fingerprints. Faces change as we age. Faces gain and lose weight, skin loses elasticity as we age, and other things from sun to laughter can deepen the lines in our faces. And while that process may be gradual, options to change a face can be instantaneous. Cosmetics (both makeup and surgery), glasses, hairstyles, masks, and inebriation all alter the way a face may appear in real-time.[151] In other words, faces just aren't consistent.

While faces are unique, they may be altered quickly or slowly and (usually) without pain or accident. Images of faces are easy to collect and store in a database. But the photo may become "outdated" with age. A face without glasses, run through facial recognition software, may measure the distance between the eyes and nose, but a photo of the same person with glasses may obscure those measurements. Faces, then, may easily fool facial recognition technology in a way fingerprints cannot.[152]

ii. PERFECT RECOGNITION REQUIRES PERFECT CONDITIONS

---

145 *Perpetual Lineup, supra* note 111, at D.1.

146 *Id.*

147 *Id.*

148 *See* Soweon Yoon and Anil K. Jain, *Longitudinal study of fingerprint recognition*, 112 PROC. NAT'L ACAD. SCIENCES 8556 (July 14, 2015) (establishing the stability of high-quality fingerprints for at least 12 years; citing anecdotal belief in stability of fingerprints over a lifetime).

149 Wilson, *supra* note 47, at 83.

150 *Perpetual Lineup*, *supra* note 111, at D.3.

151 *Id.*

152 *Id.*

Aside from physical changes, accuracy is also affected by the image quality. Much like the brain, what facial recognition technology "sees" depends on the environment in the photo.[153] The quality of the camera, the lighting in the environment, and the angle of the photo reduce the accuracy of a facial recognition tool.[154]

Cameras and video recorders vary in quality, though they are no doubt better than ever before. Still, the quality of an image will determine the accuracy of the facial recognition tools' results.[155] Algorithms struggle particularly with mixing photos from different sources—comparing a mug shot to a video, for example.[156] This is in part because the quality of the cameras may differ.[157] Low-resolution images produce particularly poor results.[158]

The environment also matters. As discussed with "the dress," lighting and background contrast can easily confuse the brain and encourage contextualization through assumptions. For facial recognition technology, lighting can be a major problem. Poor or uneven lighting can change the accuracy of a facial recognition tool by up to 40%.[159] Facial recognition

---

153 *See, e.g.*, P. Jonathon Phillips et al., *An Introduction to the Good, the Bad, & the Ugly Face Recognition: Challenge Problem*, NAT'L INST. OF STANDARDS & TESTING 346 (2011) https://www.nist.gov/system/files/documents/itl/iad/ig/05771424.pdf.

154 *Perpetual Lineup*, *supra* note 111, at D.1.

155 *Id.*

156 *Id.*

157 *See* PATRICK GROTHER & MEI NGAN, FACE RECOGNITION VENDOR TEST (FRVT): PERFORMANCE OF FACE IDENTIFICATION ALGORITHMS, NIST INTERAGENCY REPORT 8009 26 (Nat'l Inst. Standards. & Tech. 2014), https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8009.pdf ("Identification algorithms yield candidate lists where the mate is sometimes not at rank 1 because . . . of difference in enrollment image . . .").

158 *See, e.g.*, Min-Chun Yang, et al., *Recognition at a Long Distance: Very Low Resolution Face Recognition and Hallucination*, *in* IEEE 2015 INT'L CONF. ON BIOMETRICS, 237–42 (2015) https://ieeexplore.ieee.org/document/7139090.

159 *Perpetual Lineup, supra* note 111, at D.1.

algorithms, as stated in Part II A, depend on measurements of the face. When shadows created by lighting or contrast challenges are present, measurements themselves may be inaccurate and produce inexact results.[160] Tools that compare skin texture are similarly confused by poor and uneven lighting.[161] Error rates are greater when two photos contain different lighting or backgrounds.[162]

What is more, facial recognition algorithms measure more accurately with frontal images.[163] The measurements are most accurate with a full view of the face.[164] The ideal comparison is a frontal image compared to a second frontal image.[165] Frontal-facing images require, of course, cooperation from the suspect. A mug shot database will provide the first frontal image necessary; however, the comparison photo could come from a number of sources. Bystanders videoing from the sidewalk and security cameras mounted from above rarely get a frontal image of a suspect.[166] They often capture the profile or top of the head.[167] Subjects, and suspects, rarely face a camera outside of mugshots.[168] Accuracy is also affected when a suspect is in motion.[169] Videos are often poorly or unevenly lit simply due to the camera's location.[170]

Accuracy also drops when the size of the comparison database increases.[171] The more photos in the search, the more likely the algorithm is to find a match based on measurements, skin texture, and so on.[172] Depending on what the algorithm prioritizes, it may return a high rank of similarities that ultimately are not a match. Remember that facial recognition

---

160 *Id.*
161 *Id.*
162 *Id.*
163 *Id.*
164 *Id.*
165 *Id.*
166 *Id.*
167 *Id.*
168 *Id*
169 *Id.*
170 *Id.*
171 *See, e.g.*, Adrienne LaFrance, *The Ultimate Facial-Recognition Algorithm*, ATLANTIC (June 28, 2016), https://bit.ly/2XJp811.
172 Brief for the ACLU as Amicus Curiae, Lynch v. State of Florida, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018) (No. 1D16-3290).

technology and algorithms do not produce a "yes" or "no" result but a rank, typically on a scale of 1 to 5, of how similar one image might be to another.[173] As the size of the database increases, the number of similarities also increases, but this does not mean that it is the same person—only that they share similar features.

In short, the most accurate comparisons come from perfect conditions. Image quality, lighting, background, motion, oblique angles, and large databases challenge the algorithm. Any variable can be enough to generate a false positive or false negative result, but in combination, they make for high rates of inaccuracy.

iii. THE ALGORITHM IS BIASED.

An algorithm doesn't see race, right? In other words, a computer would not misidentify a minority simply because it cannot make a cross-race identification. The process appears to be more complicated than that. Research suggests that algorithms used in facial recognition technology actually do show signs of bias.[174] They perform poorly when identifying women and racial minorities—especially black people.[175] The problem is especially apparent when images suffer in quality, angle, or lighting.[176]

Facial recognition technology misidentifies black people, young people, and women at higher rates than white people, older people, and men. In fact, during a recent test in Congress, a facial recognition algorithm misidentified 28 members.[177] The photographs of the Congress people triggered matches for mug shot photos from a database.[178] People of color comprise nearly 20% of Congress but nearly 40% of the 28 false matches identified.[179] In a 2012 FBI-coauthored study, all three

---

[173] *Id.*
[174] *Perpetual Lineup*, *supra* note 111, at E.1.
[175] *Id.*
[176] *Id.* at E.
[177] Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (July 26, 2018), https://bit.ly/2OkETHe.
[178] *Id.*
[179] *Id.*

algorithms subjected to tests were 5-10% less accurate on African Americans than Caucasians.[180] In other words, if police are using a system that returns a few top matches, and the probe photo is one of an African American, the system is more likely to fail to identify the right person. This increases the risk of innocent people being bumped up the list—and thus investigated.[181] If the accurate match is pushed a few spots lower on the list, innocent people will look like better matches.[182]

How is the algorithm biased? Unfortunately, part of the problem lies in the development of technology. This includes photograph technology and algorithms.

a. LIGHTING AND CONTRAST, AGAIN.

When comparing a photo of a minority, the need for the "perfect" photograph or still image becomes critical. The problems of image quality, lighting, and database size of facial recognition software is exacerbated by minorities, especially black people.[183] This may surprise those who expect an algorithm to eliminate bias easily.

Photographs often fail to show contrast when an African American is the subject.[184] Film chemistry developed without diverse skin tones in mind.[185] Beyond the chemistry,

---

[180] *See* Brendan F. Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 IEEE TRANSACTIONS ON INFO. FORENSICS & SEC. 1789, 1797 (Oct. 8, 2012), https://ieeexplore.ieee.org/document/6327355 (hereinafter "Klare et al.").

[181] *Perpetual Lineup*, *supra* note 111, at E.

[182] *Id.*

[183] Brief for the ACLU as Amicus Curiae, Lynch v. State of Florida, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018) (No. 1D16-3290).

[184] *Perpetual Lineup*, *supra* note 111, at E.

[185] Kaitlyn McNab, *Why the Myth That Dark Skin is Harder to Photograph Persists*, ALLURE, (Nov. 2, 2021), https://www.allure.com/story/photographing-darker-skin-tones (This is not to say that black skin is at all hard to photograph in 2022, but that most photographers believe the myth as the trouble originated in the 1940s and fail to consider the needs of minorities when editing and photographing.).

developers never considered balancing photos for diverse populations.[186] From the 1940s until the 1990s, Kodak, a leading producer of film, supplied photo labs developing pictures with a reference card (called a "Shirley card") for skin tones.[187] The card featured Shirley, a Kodak employee with light skin and brunette hair.[188] This became the standard for color correction.[189] As a result, lighting, shadow, and contrast in the film were subpar for minorities, especially African Americans.[190] This problem persists. An MIT study noted that digital cameras and video fail to provide the contrast a facial recognition algorithm needs to produce and match faces.[191]

If a facial recognition tool is affected up to 40% by poor lighting, contrast, database size, or lack of frontal image, the problem is compounded when an African American person is photographed and the contrast, lighting, or image quality is poor. The need for a well-lit, high-contrast photo with the subject directly facing the camera is even greater for those the algorithm struggles to measure because of race.

As described earlier, facial recognition algorithms depend on measurements of facial features. The quality of the photo influences the accuracy of a match. A photo that is poorly lit or lacks contrast for sufficient detail is more likely to result in misidentification. A good image is vital because the algorithm may struggle to identify minorities if it lacks sufficient data for comparison, too.

b. LACK OF EXPERTISE, AGAIN.

Computers, unlike humans, do not grow up and remain in de facto segregated communities—but the algorithm is only as good as its dataset.[192] Facial recognition technology software is trained to identify and match photos. These systems "learn"

---

[186] *Id.*
[187] *Id.*
[188] *Id.*
[189] *Id.*
[190] *Id.*
[191] *See* Klare, et al., *supra* note 180, at 1789-1801.
[192] *See* Klare, et al., *supra* note 180, at 1789-1801.

to identify faces based on previously identified images.[193] Images are then trained to identify and distinguish the population in the dataset.[194] If the algorithm is trained using a population that does not represent the population targeted during deployment, accuracy rates plummet.[195] Indeed, much like cross-race identification, a system trained with Caucasian images performs best on Caucasian probe photos. The same is true for algorithms trained with African American or Latino datasets; each performs better on the race in which it is trained.[196]

How, then, are most facial recognition technologies "trained"? Most use celebrity photos. Microsoft, in particular, used thousands of images of celebrities to develop facial recognition technology.[197] The database also collected images of scholars and activists. Microsoft removed the database from the internet after public concern arose around other countries, including China, purchasing the repository and developing facial recognition software.[198] Stanford University conducted a study at a café called Brainwash.[199] Cameras captured thousands of faces in the café and added them to a dataset to develop facial recognition algorithms.[200] Duke University created a similar repository.[201] Websites and applications like Facebook and TikTok also encourage users to upload photos or videos to "find a celebrity match."[202] This simultaneously

---

193 *Perpetual Lineup, supra* note 111, at E.2.

194 See Klare, *supra* note 180, at 1800 ("Face recognition performance on race/ethnicity . . . generally improves when training exclusively on that same cohort.").

195 *Id.*

196 *Id.*

197 Madhumita Murgia, *Microsoft Quietly Deletes Largest Public Face Recognition Data Set*, FIN. TIMES (June 6, 2019), https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2.

198 *Id.*

199 *Id.*

200 *Id.*

201 *Id.*

202 Megan McCluskey, *TikTok Has Started Collecting Your 'Faceprints' and 'Voiceprints.' Here's What It Could Do With Them*, TIME MAGAZINE (June 14, 2021 12:45 PM), https://time.com/6071773/tiktok-faceprints-voiceprints-privacy/.

creates a dataset and trains the software. To say the least, this fails to capture the full range of human diversity.

The previously cited MIT study found that two datasets used to train facial recognition algorithms were "overwhelmingly composed of lighter-skinned subjects."[203] The algorithm, then, had little experience or expertise in examining racial minorities, especially black people, and the accuracy fell significantly.[204]

In short, facial recognition software fails to capture the full range of human characteristics, and the algorithm's training and dataset suffer.

c. FREQUENCY OF CONTACT

Facial recognition technology can only find a match in the database it searches.[205] This seems obvious but is important to note. Law enforcement agencies often use mugshot databases. The problem with inaccuracy may be compounded because black people experience disproportionate interactions (and arrests) with the police.[206] Disproportionate interactions create a population that is then more "findable."[207] Facial recognition technology underperforms in the identifications of black people, yet we are asking the algorithm to perform these searches more often.[208]

Further, using a mugshot database may result in an overrepresentation of black people to use as comparison data. As discussed above, accuracy rates plummet when the size of the database increases, no matter the race of the person in the probe photo or the dataset used for training. But if the database includes a mugshot database that disproportionately features African Americans because of the disparate interactions with police, cause for serious concern arises. Accuracy is affected by frequency of contact, and African Americans are overrepresented in the mugshot databases in most cities.[209]

---

[203] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. OF MACH. LEARNING RSCH. 77 (2018), https://bit.ly/2Ek9ZwZ

[204] *Id.*

[205] *Perpetual Lineup, supra* note 111, at E.3.

[206] *Id.*

[207] *Id.*

[208] *Id.*

[209] *Id.*

The algorithm itself is only as good as its dataset. The image quality, lighting, and contrast of a photo influence the quality of match results. What is more, the algorithm's training results in a level of expertise that limits the effectiveness of identification across races. Finally, the dataset itself may be "too extensive" with respect to African Americans. In other words, the dataset may overrepresent a population that is particularly prone to inaccurate identifications, giving even more opportunities for misidentification in that population. The bias is evident.

iv. IMPLICIT BIAS IN A MACHINE?

Of course, algorithms do not operate alone. Most departments using facial recognition technology also have a human reviewing the results.[210] These individuals can correct an inaccurate identification and prevent harm. A human reviewer can bolster accuracy by interpreting results, communicating results and what they signify (not a "yes" or "no" answer) to members of law enforcement, and finding obvious errors. Essentially, a reviewer can know that seeing is not always believing.

Regardless, the National Institute of Standards and Technology's research shows that humans are likely to believe the computer-generated results.[211] Simple human review is inadequate.[212] As discussed above, humans are generally poor sources of identification. Those without special training in facial recognition are doomed to fall victim to the problems of human identification identified in Part I. This risks putting the bias back into the system. Those without special training are particularly inept at noticing a difference in cross-races. Even a person with special training misidentifies a subject about 10% of the time.[213]

---

[210] *Id*. at D.

[211] *Id*. at D.3.

[212] *Id.*

[213] P. Jonathon Phillips et al., *Face Recognition Accuracy of Forensic Examiners, Superrecognizers, and Face Recognition Algorithms*, PNAS (May 29, 2018), https://bit.ly/2VGgaji; David White, et al., *Error Rates in Users of Automatic Face Recognition Software*, PLOS ONE (Oct. 14,

The 2016 Georgetown study found that some agencies have training for analysts, but only eight systems reported employing human supervisors to review matches before forwarding them to officers.[214] Of the eight that do employ supervisors, the training is unclear and not standardized.[215] The risk of facing implicit bias varies from jurisdiction to jurisdiction.

v. THE RISK BECOMES REALITY.

Misidentification in facial recognition technology is not just a risk—it is a reality. On January 9, 2020, almost one year before the Capitol Riots of 2021 and the uptick in facial recognition software use, Robert Williams was arrested by the Detroit Police Department on his front lawn, in front of his family.[216]

Facial recognition software identified Mr. Williams as the perpetrator of a watch heist from a Shinola store.[217] A security guard at the store observed footage of an unidentified Black man stealing five watches inside the store.[218] The surveillance video is poorly lit and never captures a frontal image of the suspect.[219] Detroit Police used facial recognition software to take an image from the surveillance footage and compared it to a database of stored Detroit driver's license images.[220] The search returned Mr. Williams' old driver's

---

2015), https://bit.ly/2TlTpVl (noting participants made over 50% errors for adult target faces).

[214] *Perpetual Lineup, supra* note 111, *at* D.2.B.

[215] *Id*.

[216] Robert Williams, *I Did Nothing Wrong, I Was Arrested Anyway*, ACLU (July 15, 2021), https://www.aclu.org/news/privacy-technology/i-did-nothing-wrong-i-was-arrested-anyway.

[217] Miriam Marini, *Farmington Hills Man Sues Detroit Police After Facial Recognition Wrongly Identifies Him*, DETROIT FREE PRESS (Apr. 13, 2021 4:31 PM) https://www.freep.com/story/news/local/michigan/2021/04/13/detroit-police-wrongful-arrest-faulty-facial-recognition/7207135002/.

[218] *Williams, supra* note 216.

[219] Complaint at 4, *Robert Williams v. City of Detroit* ECF No. 1, 2:21-cv-10827-GAD-APP (E.D. Mich. 2021) [hereinafter, Complaint].

[220] *Williams*, *supra* note 216.

license photo as one of the "top" matches.[221] Detroit police placed Mr. Williams' photo in a lineup, and the security guard selected the photo.[222] The DPD called Mr. Williams and asked him to report to the station to be arrested for the theft charge.[223] When Mr. Williams asked for more information, the officers threatened to come to his place of work to carry out the arrest.[224] Instead, Mr. Williams told them he was headed home and would speak to them there.[225] Once at the home, officers handcuffed Mr. Williams on his front lawn before he could go inside.[226] Taken to the Detroit Detention Center, he was held overnight.[227] The next day, during an interrogation, an officer showed Mr. Williams the security footage that led to the facial recognition "match."[228] When comparing Mr. Williams's face to the photo, it became evident that officers based the arrest on an erroneous facial recognition identification.[229] The officer, confused, looked at Mr. Williams's face, comparing it to a still image of the security footage. "I hope you don't think all Black men look alike," Williams said.[230] The officer told him, "I guess the computer got it wrong."[231] Williams waited a few more hours before his release. Eventually, the charges against Williams were dismissed.

Mr. Williams' wrongful arrest based on inaccurate facial recognition data is often called the first *known* of its kind in the United States. Recently, the Detroit Free Press found out that it was the second.[232] A 25-year-old Detroit resident, Michael

---

221 *Id.*
222 *Id.*
223 *Id.*
224 *Id.*
225 *Id.*
226 *Williams*, *supra* note 216.
227 *Id.*
228 Victoria Burton-Harris & Phillip Mayor, *Wrongfully Arrested Because Facial Recognition Can't Tell Black People Apart*, ACLU (June 24, 2020), https://www.aclu.org/news/privacy-technology/wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart.
229 *Id.*
230 *Id.*
231 *Id.*
232 Elisha Anderson, *Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit*, DETROIT FREE PRESS (July 11, 2020 11:03 PM)

Oliver, was accused of a felony for allegedly smashing a car window, grabbing a cell phone, and smashing it on the ground.[233] Detroit Police used facial recognition technology to develop an investigatory lead.[234] After the software returned a photo of Mr. Oliver as a potential match, the victim identified him in a lineup.[235] Mr. Oliver insisted he was innocent.[236] Evidence supported his claim.[237] The perpetrator in the cellphone video used to probe the database for matches had no tattoos visible on his arms.[238] Mr. Oliver's arms have several tattoos.[239] Eventually, the charges against Oliver were dismissed.[240]

These two cases, the first and second *known* cases of misidentification using facial recognition technology, are cases of faulty detective work, according to Detroit Police. In Mr. Williams's case, the Detroit Police Department acknowledged that what should have been used as an investigative lead was used as probable cause to arrest.[241] The Detroit Police Department wanted to search a database for matches on the Shinola surveillance video but did not have a facial recognition analyst on duty that day.[242] The department contacted the Michigan State Police, who ran still images of the video against a database containing images of mugshots, driver's license photos, and unsolved crimes.[243] Mr. Williams's photo returned as a match—ranked ninth-best.[244] Rather than using the lead to develop an investigation, a detective showed the photo to the Shinola security guard.[245] That guard had only seen the

---

https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/.

[233] *Id.*

[234] *Id.*

[235] *Id.*

[236] *Id.*

[237] *Id.*

[238] Anderson, supra note 232.

[239] *Id.*

[240] *Id.*

[241] Marini, *supra* note 217.

[242] Williams Compl., *supra* note 219, at 69.

[243] *Id.*

[244] *Id.*

[245] Anderson, *supra* note 232.

surveillance video—not the incident—and the incident occurred more than a year earlier.[246] Officers omitted this information when applying for the arrest warrant.[247]

vi. PROTECTING ACCURACY, PREVENTING MISIDENTIFICATION.

The Williams and Oliver cases highlight the importance of accuracy and training when police use facial recognition technology as an investigative tool. The persuasive, powerful nature of the technology demands a working knowledge of the tool and its limitations to properly wield such a weapon.

It seems that facial recognition technology, while not new, is young and less understood. As a result, accuracy may be a lesser-protected value, and the limitations of the technology may not be widely known or understood.

a. PROCUREMENT AND STANDARDS.

First, agencies do not regularly consider accuracy when purchasing third-party software. During the 2016 Georgetown study of facial recognition technology and law enforcement agencies, few agencies responded to requests to provide contracting documents.[248] Of the nine that did respond, four purchased facial recognition software without a competitive process to compare products.[249] Some, like the Los Angeles County Sheriff's Department, did not require any demonstration of accuracy in the software.[250] Some agencies, like the San Francisco Police Department, permitted bidding and required specific accuracy targets from each company.[251] Little transparency and consistency exist in the acquisition of the technology and its performance requirements.[252]

Accuracy, then, turns on the jurisdiction and the purchasing choice by the local law enforcement agency. Departments that value a lower price may tolerate a higher

---

246 *Id.*
247 *Id.*
248 *Perpetual Lineup*, *supra* note 111, at D.2.
249 *Id.*
250 *Id.*
251 *Id.*
252 *Id.*

error rate, decline comparing accuracy tests conducted by an independent source, and fail to verify accuracy promises with their tests and detect degradation.

b. SPECIALIZED TRAINING.

Human review is an essential component of facial recognition technology as a law enforcement tool. While a human already inputs the probe image and compares the results, a human must also interpret those results to ensure accuracy. As we have discussed, humans are poor judges of facial similarities. Specialized training can eliminate some mistakes that humans make in recognizing faces. Specialized training can increase accuracy in facial recognition by 20%.[253]

While training improves accuracy, only eight responses to the Georgetown study revealed a policy of human gatekeepers reviewing matches before forwarding them to officers.[254] What is more, the level of training the human gatekeepers in these eight agencies might receive is unclear and not standardized.[255] When a state contacts the FBI to conduct a search, the FBI returns results to the department with no human review.[256] Training varies from department to department. Policies are generally not made public, and the process appears shrouded in secrecy.

Unfortunately, this shortcoming took center stage in a Florida case questioning whether facial recognition technology use and results are *Brady* material. In *Lynch v. Florida*, police used the FACE Services facial recognition software to identify a man who purchased drugs from undercover agents.[257] The agents snapped a grainy, poorly lit photo of the buyer and a data analyst used the cell phone snap as a probe photo to compare to the FACE database.[258] The system identified Willie Allen Lynch as a potential match with one star.[259] At a pretrial deposition, the data analyst responsible for operating the FACE

---

[253] *Id*. at D.2.B.
[254] *Id*.
[255] *Id*.
[256] *Id*.
[257] Lynch v. State, 260 So. 3d 1166, 1169 (Fla. Dist. Ct. App. 2018).
[258] *Id*. at 1168-1169.
[259] *Id*. at 1169.

program and inspecting the results implicating Willie Allen Lynch admitted she did not know how the system rates photos.[260] While she acknowledged the system returned results between one and five stars, she was unsure whether one star was the best match or five stars suggested the most similarities.[261] She could not articulate what a star rating suggested (a significant similarity, not a "yes" or "no" result).[262] Other officers testified that they accepted the results of the FACE search in the *Lynch* case at face value and did not continue the investigation.[263]

c. A LACK OF TRANSPARENCY.

Most agencies do not reveal much about the use of facial recognition technology as an investigative tool. Much of what is known is achieved through investigative journalism, such as the cases of Mr. Williams and Mr. Oliver in Detroit. Thousands of database searches take place with the FBI alone. What is more, while concerning that the public remains unaware of the tools agencies may deploy in an investigation, or their appearance in a database used to identify suspects, those who are identified by a facial recognition software product in a criminal investigation may never know.[264] While departments use facial-recognition software to develop leads and begin investigations to obtain probable cause to arrest, criminal defendants are not entitled to this information as a *Brady* disclosure.[265] If the software identified someone other than the criminal defendant in a case, the defendant may never know and cannot present that information in mounting a defense.

Because facial recognition technology is part of the investigative process and not subject to disclosure, and because

---

[260] *Id*.
[261] *Id*.
[262] *Id*.
[263] *Id*.
[264] Brief for the ACLU as Amicus Curiae, *supra* note 172 (". . . among the thousands of cases in which the state uses FAES each year, this appears to the be the only unreported case in Florida addressing the use of the system . . . That suggests widespread failure to disclose . . . use of FACES to defendants and courts.").
[265] *Lynch*, 326 So. 3d. at 1172.

it is often used before Fourth Amendment safeguards may trigger, little oversight of agencies using this powerful tool exists. Few agencies inform the community about the existence of facial recognition technology, and fewer tell the communities how and when they use it.[266] Only one agency, as of 2016, informed the public of how often it uses facial recognition technology.[267]

IV. PART III. MAN AND MACHINE: NOT THAT DIFFERENT AFTER ALL.

At first blush, one might think that the risks of eyewitness identification can be avoided or, at the very least, mitigated by using an algorithm in facial recognition technology. The conclusion may be tempting because humans are error-prone and biased, but the proper conclusion is that eyewitness identification and facial recognition technology share more in common than first expected.

A. BOTH ARE SO PERSUASIVE.

Eyewitness identification and facial recognition technology both risk overreliance by a jury. Eyewitness identification is persuasive. Jurors and other actors in the criminal justice system are likely to believe eyewitness identification because it is historically valued and because we tend to believe our own memories are infallible. Similarly, jurors (should they ever learn about facial recognition technology in an investigation)[268] and others in the criminal justice system are likely to trust a computer more than a human. In fact, the amount of trust a human places in an algorithm increases with the complexity of the problem. As communities learn of the limitations and risks of eyewitness identification, especially racial bias, the natural tendency may be to lean into facial recognition algorithms as a solution. All the same, no algorithm is infallible. Any belief that an algorithm can produce

---

[266] *Id*.

[267] *Perpetual Lineup*, *supra* note 111, at A.2.

[268] This supposes that a jury would hear evidence of facial recognition technology's role in the investigation, but that is increasingly less likely as courts determine facial recognition algorithm results are not *Brady* material.

a "yes" or "no" prediction in face recognition is impractical. Facial recognition algorithms are merely a tool, not a solution to the problem of identification. Facial recognition technology should be approached with the same skepticism one might approach with eyewitness identification. There should be an emphasis on reliability and accuracy and practices to avoid misidentification.

B. BOTH ARE SO INACCURATE.

Eyewitness identification and facial recognition technology both produce inaccurate results. The factors that cause the inaccuracies are shockingly similar. First, the environment in which an event occurs and from which an eyewitness can observe matters. Eyewitnesses may be unable to accurately recall an event when there is poor lighting, obstructed views, or suspects wear glasses, masks, or make other alterations to their appearance. Furthermore, viewing a still image runs the risk of inaccurate identification based on backlighting, lack of context, and other factors that encourage the human brain to "fill in" the details. Finally, the stress of an event, the angle at which a person observes the event, and the length of time between the event and recall all alter a memory and one's recall ability. The human memory is not, after all, an instant replay video.

Facial recognition technology faces the same challenges. The quality of the probe photo and the quality of the dataset photos can affect accuracy. Poor lighting, obstructed angles (views that are not frontal), and poor resolution can limit the algorithm's ability to measure facial features. Further, color contrast challenges exist with respect to African American photographs. What is more, the length of time between the probe photo and the dataset photo can have catastrophic effects on the algorithm's accuracy. As a person ages, facial features change. Skin texture, lines, and skin elasticity are not static. Further, glasses, makeup, and hairstyles affect the algorithm's accuracy. Even a computer is not infallible. Both eyewitness identification and facial recognition technology require the perfect condition for the perfect identification. This means frontal images, taken in perfect lighting, unobstructed, and with little time between the event and the recall or inquiry. Perfect conditions, like perfect people or perfect algorithms, do not exist.

C. RACIAL BIAS IN HUMANS AND ALGORITHMS.

Perhaps the most concerning challenge both humans and facial recognition software face is that of cross-race identification. We now know eyewitnesses often erroneously identify members of cross-races because they lack expertise with faces in that race. *De facto* segregation persists in the United States, and we may have less opportunity to interact with members of a cross-race. Therefore, we consciously or unconsciously fail to notice distinguishing features. We may use broad categories to identify an individual and later fail to recall specifics with great accuracy or detail.

What is surprising, though, is that algorithms in facial recognition technology suffer the same shortcomings. While they are not "living" in a *de facto* segregated society, they receive training. The training determines how well the product will perform. When the training images do not contain a sufficiently diverse population, the same cross-race misidentification problem emerges. Facial recognition algorithms exposed in training to one race identify members of that race with greater accuracy, just like a human might notice distinguishing characteristics with more accuracy.

The risk in replacing or hoping to replace inaccurate eyewitness identifications plagued by cross-race identification challenges is that algorithms may fare no better. We should not think of a computer as free of bias and should not rely on algorithms as an investigative tool to reduce bias. We must operate with the understanding that we must still guard against and mitigate the risk of bias with facial recognition technology.

D. EYEWITNESS IDENTIFICATION HAS A SLIGHT EDGE.

Surprisingly, eyewitness identifications may have a slight edge in accuracy and reliability. The Supreme Court elected to step in and fashion a test to examine the totality of the circumstances to ensure an emphasis on reliability, recognizing some eyewitness identifications are inaccurate. The *Manson* factors make sure that eyewitness identifications can be considered by the finder of fact, so long as there is sufficient indicia of reliability.[269] *Manson* prevents a per se rule against

[269] *Manson*, 432 U.S. at 112.

eyewitness identification that would stymie police investigations, make it difficult to develop leads in cases, and ultimately keep good evidence away from the jury.[270] Eyewitness identification has the benefit of time. Recounting experiences is historically valued and is a bedrock of most court proceedings. The Court worked hard to respect the need for, while acknowledging the limitations of, eyewitness testimony and identification. Today, the body of case law addressing eyewitness identification is extensive. In fact, police agencies design policies related to eyewitness identification scenarios like lineups and show-ups to ensure reliability and prevent misidentifications.

Facial recognition technology, on the other hand, while not new, is young. The first use occurred in 1990.[271] Technology is ever-changing and ever-improving in capabilities. It is hard to know when a new tool can perform the task at hand well or is just capable of performing the task at hand with no regard for accuracy. Given the secrecy of the use of facial recognition technology, coupled with the fact that most deployments of facial recognition software occur before a search warrant, arrest warrant, or any other event that might trigger judicial review, there have been few opportunities to implement rules like those in *Manson* that might discourage the use of inaccurate results while preserving the ability to use sufficiently reliable and accurate results to develop an investigation. As a result, few rules guiding the use of facial recognition technology exist. Police agencies have few policies related to the use of facial recognition technology. Of the policies that are present, they remain unpublished. What is more, the policies are not standardized across jurisdictions.

Given the similar challenges that eyewitness identifications and facial recognition technology share, and considering the lack of rules and policies that operate to ensure reliability in human identifications, legislatures, law enforcement agencies, and courts should work to fashion a solution. Minimizing misidentifications protects the public and builds trust between law enforcement and the public. What is more, solid policies and laws would permit police to use a valuable tool to develop leads and investigate crime while still mitigating the risk of misidentification. Without oversight and

---

[270] *Id.*

[271] *Perpetual Lineup*, *supra* note 111, at III.C.

strong examination as to the accuracy of the tool, the accuracy of investigations and the public's confidence in arrests and convictions will be questioned.

V. PART IV. THROW OUT THE BATHWATER, KEEP THE BABY: SOLUTIONS TO MINIMIZE THE RISKS.

In crafting a solution to the challenges of eyewitness identifications, the Court did not seek to establish a per se rule that eliminated all use of the risky tool. Indeed, the Court acknowledged that there is often no better evidence than eyewitness testimony, so long as it is sufficiently tested for reliability. Addressing the challenges of facial recognition technology should acknowledge the same principles. The tool, if reliable, is valuable and can aid the police in developing leads, investigating crime, and protecting the public; however, the tool must be reliable, unsuggestive, and only used as part of an investigation. The tool cannot and should not be the only piece of an investigation. Law enforcement agencies should establish policies about the procurement of facial recognition tools, the deployment of such tools in an investigation, and training for experts who examine generated results. Further, law enforcement agencies should report instances of the use of facial recognition technology in an annual report since most deployments are pre-Fourth Amendment deployments that may not be apparent to the public. Finally, federal agencies should lead the way toward written policies, demands for accuracy, and accountability. Written policies, proper oversight, partnership, and reporting will permit a valuable tool to remain in the hands of the police while also guarding against misidentification.

A. LAW ENFORCEMENT SHOULD HAVE WRITTEN POLICIES ABOUT FACIAL RECOGNITION TECHNOLOGY.

Accountability and responsibility begin with identifiable standards. Law enforcement agencies should develop and implement standardized policies related to facial recognition technology and its deployment in a community. Written policies serve to bring uniformity to any process. With facial recognition algorithms, written policies can promote the accuracy of results and mitigate the risk of misidentifications. Written policies can cover the procurement of software that

meets the minimum acceptable level of accuracy and performance, can prevent misuse of the technology when an officer relies on the identifications without other evidence to suggest reasonable suspicion, and establish a minimum level of training for analysts. Written policies that address these concerns should be published in the communities that law enforcement agencies serve. Informing the public serves to hold law enforcement agencies accountable to meet the suggested standards, builds public trust, and allows oversight.

i. LAW ENFORCEMENT SHOULD PROCURE SOFTWARE WITH A HIGH ACCURACY RATE.

First, law enforcement agencies should establish a policy for the procurement of facial recognition software. Procurement policies should discourage contracting with a private software company without examining multiple products from several companies to promote competition, not just in price but in performance. The written policy should consult National Institute of Science and Technology standards for accuracy in facial recognition algorithms, should be examined often for improvements, and should have a specific target in mind before accepting bids. The public should know the target accuracy or performance standard and be aware of justifications for this standard.

In examining procurement, agencies should require bidding private companies to reveal the dataset used to "train" the algorithms, ensuring the community and the dataset are similar in demographics to promote accuracy across races.

ii. LAW ENFORCEMENT SHOULD ONLY USE FACIAL RECOGNITION TECHNOLOGY IN TANDEM WITH OTHER INFORMATION IN AN INVESTIGATION.

The stories of the Detroit Police's misuse of facial recognition technology in the cases of Robert Williams and Michael Oliver are startling. The examples show what might happen when facial recognition algorithms suggest similarities in photos and an investigator fails to fully explore the lead, gather other information or evidence, or rely on other evidence to obtain an arrest warrant. In the world of sports, instant replay is used to confirm what an official sees with his or her own eyes.

Then, the official makes a judgment call and uses video to confirm or deny that observation. Facial recognition technology should work in the same manner. An investigation should lead to reasonable suspicion, and facial recognition software should confirm or deny that observation. The software itself should not make the initial and only observation. Misidentification has a significant risk of depriving an innocent person of his or her liberty, and so facial recognition technology should never be the sole piece of evidence in a case.

Law enforcement agencies should implement written policies that address the need to use facial recognition software to enhance an investigation rather than as the entire investigative process. A written policy that requires other corroborating evidence before obtaining an arrest warrant for a person identified by facial recognition software is essential to prevent judgments made in a hasty fashion, prevent misidentification based on inaccurate software, and prevent unnecessary deprivations of liberty.

iii. LAW ENFORCEMENT SHOULD TRAIN EXPERTS USING FACIAL RECOGNITION TECHNOLOGY.

Because there is a risk of liberty and privacy deprivation with the use of facial recognition software to develop leads in investigations, it is important to train the analysts using this software. The *Lynch* case is particularly shocking when considering analyst training. The analyst in the case could not discuss how the system operates, what a result might suggest, or whether the scale operated with one as the highest or lowest match. Human analysts are the stop-gap that prevents an algorithm that may have poor accuracy with regard to photos that are unclear, poorly lit, or feature low contrast. Analysts are also the stop-gap that prevents an algorithm that struggles to analyze African American faces. When analysts cannot properly recognize what an algorithm is testing, how the result should be interpreted, and whether there is a risk that the result is inaccurate, the analyst cannot effectively eliminate bad matches. What is more, an analyst unfamiliar with the system cannot communicate the limitations of the software to others relying on the data—investigators, detectives, and officers seeking warrants.

A written policy and standardized training can ensure those acting as the human fail-safe against algorithm inaccuracy

perform effectively. In addition, a written policy protects the liberty and privacy of the public and communicates the need to develop more leads and discover more evidence before obtaining an arrest warrant or formally charging an individual. A written policy and standardized training are some of the most important things an agency can do to build public trust in using such a powerful tool.

iv. THE POLICIES SHOULD BE SUBJECT TO LEGISLATURE OR PUBLIC REVIEW.

A law enforcement agency should submit the written policies for the use of facial recognition technology to a local or state legislature for review and allow public comment. Police cannot operate in a vacuum, and while agencies are best positioned to understand the needs of police in using a tool during an investigation, local or state legislatures and the public are uniquely positioned. Legislatures and the community itself are more capable of describing the needs of the community, the impact a tool may have, and the perception the public has toward the tool's use. The relationship between the public and the police is important. Particularly, a strong relationship of mutual trust promotes public safety, and partnership can make policing safe and effective. When the public understands facial recognition technology and its use and understands the parameters in which the police will operate, a higher level of trust is created. Written policies that consider the impact on the community build trust, as does the ability to hold agencies accountable to adhere to the policies. This open dialogue and communication seem so simple but are so effective. The benefit of public comment on a facial recognition technology policy cannot be overstated.

B. LAW ENFORCEMENT SHOULD CONDUCT INTERNAL AUDITS TO SHOW FREQUENCY OF USE.

Facial recognition technology is so powerful, it simply cannot be kept secret. Deployments of facial recognition software occur most in the pre-investigation stage before a Fourth Amendment right is triggered. As a result, courts have limited opportunities to craft rules to guide the use and ensure police accountability and oversight. To that end, agencies should be made to compile

data and publicly report the deployments of facial recognition technology. This should include the number of facial recognition searches run, the crimes those searches were used to investigate, the arrests and convictions resulting from these searches, and what databases an agency access. Using this information, the public can remain informed about how the community uses facial recognition technology is used, who the technology may target, and how law enforcement uses the technology to investigate and develop leads in criminal investigations. Along with providing data and examples to use, public reporting provides one more layer of accountability that builds public trust.

Additionally, law enforcement agencies should conduct internal audits of their facial recognition software's accuracy. These reports should be conducted regularly, published, and disseminated, so the public is aware of the software, its capabilities, and whether the software's accuracy matches industry standards.

Auditing and publishing reports may take time, resources, and manpower from an agency, but the public trust gained from this energy is a good use of department resources. State and local legislatures should consider funding for these audits as part of the allocation of tax dollars to ensure accountability.

C. FEDERAL AGENCIES SHOULD LEAD THE WAY

The FBI accesses many state databases to compare photos and gathers datasets from many more. What is more, other agencies, including the IRS and Social Security Administration, are considering implementing facial recognition technology. To encourage agencies at the state and community level to implement written policies, disclose policies to the public, and demand accuracy from private companies, federal agencies should set the tone with their own policies.

Federal agencies partner with many state and local agencies to allow access to FACES Services. Federal agencies often take a probe photo from a state agency and compare it to the federal databases. The federal agencies should have strict accuracy expectations, written policies requiring individualized suspicion, and special training for analysts who produce results as requested by state and local agencies. By

demanding accurate, reliable algorithms and providing a knowledgeable analyst to interpret results, federal agencies could emphasize the importance of partnership. What is more, the transparency would serve as an example to the state and local agencies of the importance and benefits of public accountability and partnership.

What is more, federal agencies should demand that state and local agencies looking to partner and exchange information follow the same expectations of accuracy in algorithms. Access to the federal databases or sharing of information with the state and local databases should require a written department policy about facial recognition technology. State and local agencies wishing to access an algorithm or share information with a federal agency should show a written policy requiring a standardized accuracy expectation for an algorithm, a need for individualized suspicion in each case, and training for analysts, detectives, and officers using information from an algorithm. Requiring a written policy could be both a carrot and stick. It would encourage compliance but also preclude departments that do not comply from accessing powerful investigative tools.

Of course, no solution is perfect, and every solution is an expense in a budget for a law enforcement agency. However, investment in accuracy and accountability can pay off in the long run through safety, partnership, and community trust. Communities and law enforcement agencies with good working partnerships are safer. The public may be willing to work with the police when an understanding exists that departments and the community share the same values and understand the unique challenges of the community; in other words, transparency and accountability matter in policing. A tool as powerful as facial recognition technology deserves to be handled with care. The benefits are many—as are the risks.

VI. PART V. CONCLUSION.

We return now to the story of Mark Simon, convicted of storming the United States Capitol on January 6, 2021. We compare this with the story of Robert Williams, wrongfully arrested in connection to a store burglary. Facial recognition technology, an investigative tool, identified both men. The investigations and discovery of individuals like Mark Simon in connection with the Capitol Riots stand to allow the public to

learn about a tool that has, until now, existed mostly in the shadows. The resulting arrests often draw the public's admiration. A quick resolution to a crime that shocks the conscience builds public confidence in facial recognition technology as an investigative tool. It normalizes the procedure and encourages extension to other crimes.

Even so, normalizing the use of facial recognition technology, without considering the solutions suggested in Part IV, risks experiences like Robert Williams had and will become the new normal. Without regulation, standards, and training, facial recognition technology may be deployed extensively across the country with little oversight. The public will have no opportunity to know how the tool is used and what impact the tool may have on communities of color. Expanding the use of this technology without appropriate agency-level policies and oversight poses a direct risk to those who are most vulnerable to harm during an encounter with law enforcement. Pursuit of Capitol Rioters with little oversight in the use of facial recognition technology, while a noble cause, risks inflicting lasting harm on minorities by normalizing an investigatory tool with little oversight, accuracy, or transparency. The ends of justice must justify the means. Until there are procedures in place to ensure this, the use of this investigatory tool should be minimal.