Duquesne Law Review

Volume 60
Number 2 *The Death of Eyewitness Testimony and the Rise of Machine*

Article 6

2022

Considering "Machine Testimony": The Impact of Facial Recognition Software on Eyewitness Identifications

Valena Beety

Considering "Machine Testimony": The Impact of Facial Recognition Software on Eyewitness Identifications

*Valena Beety**

INTRODUCTION

Andrea Roth's seminal work in *Machine Testimony* and *Trial by Machine* presented a problem that is now upon us: addressing biased algorithms and the rampant reliance on technology by prosecutors and law enforcement.[1] That reliance, however, is no longer unquestioning. Roth's work came at a crucial moment in time, when other articles were embracing the apparent impartiality of technology and algorithms for use in the criminal legal system. Her scholarship steered us away from that blind acceptance and dove deep, not only questioning technology itself, but also *how to frame* those questions of technology in the courtroom.

Machine Testimony combined the acumen of a far-seeing scholar with a practitioner's on-the-ground practicality. The piece looked deeply at how the rules of evidence, pre-trial disclosure, and corroboration should apply to developing forms of technology.

---

* Professor of Law, Arizona State University Sandra Day O'Connor College of Law; Deputy Director, Academy for Justice. I cannot thank Professor Jane Moriarty enough for organizing this valuable symposium and bringing us all together as scholars and colleagues. Thank you also to the 2021 ABA Criminal Justice Section Academics Committee Work-In-Progress Roundtable, and for elucidating feedback from Professors Shirin Bakhshay, Deborah Denno, and Margareth Etienne. Finally, thank you to editor Nakib Kabir who brought out the best in this piece.

1. Andrea Roth, *Machine Testimony,* 126 YALE L.J. 1972, 1972 (2017).

Roth importantly identifies some machine findings as testimonial evidence.[2] She writes: "Both physical and testimony evidence can lead to decisional inaccuracy[,]" but "[t]estimonial evidence presents different challenges for decisional accuracy.[3] Even if the factfinder's powers of observation and inference are working well, she might draw an improper inference if the source is not worthy of belief."[4]

One case in point is machine modes of identification. Research has widely demonstrated the decisional inaccuracy that results from unreliable identifications, either by human eyewitnesses, or facial recognition software.[5] Wrongful convictions can occur when police use either of these identification methods without precautions. Contextual information is vital to whether a factfinder correctly interprets either type of evidence.

This Article uses a wrongful conviction lens to compare identifications by machines, notably facial recognition software, with identifications by humans. The Article advocates for greater reliability checks on both before use against a criminal defendant. The Article examines the cascading influence of facial recognition software on eyewitness identifications themselves and the related potential for greater errors. As a solution, the Article advocates the inclusion of eyewitness identification in the Organization of Scientific Area Committees' ("OSAC") review of facial recognition software for a more robust examination and consideration of software and its usage. The Article also encourages police departments to adopt double-blind procedures for eyewitness identifications, including when "matching" photos from facial recognition software are included. Finally, the Article concludes with a prediction of where these two fields will be ten years from now, in 2032.

I. UNRELIABILITY OF EYEWITNESS IDENTIFICATION

Courts would rarely admit eyewitness identifications if based on their scientific reliability. Few types of evidence are as unreliable as human identifications, yet they are routinely admitted in court.[6]

---

2. *Id.* at 1984.
3. *Id.*
4. *Id.*
5. *See generally*, Aliza B. Kaplan & Janis C. Puracal, *Who Could It Be Now? Challenging the Reliability of First Time In-Court Identifications After* State v. Henderson *and* State v. Lawson, 105 J. CRIM. L. & CRIMINOLOGY 947 (2015); Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1210 (2021).
6. *See generally* Kaplan & Puracal, *supra* note 5, at 947.

Prosecutions frequently depend on an eyewitness to secure a conviction.

The decreased reliability of eyewitness identifications is partially due to a lack of effective standards. In 2011, the New Jersey Supreme Court crucially and influentially adopted robust protections to heighten the likelihood of a valid identification.[7] In *State v. Henderson,* the New Jersey Supreme Court relied on decades of scientific research to reform and strengthen its test for admissibility of eyewitness identification evidence, addressing influential factors that were "within the control of the criminal justice system," namely human factors.[8]

But a year following the *Henderson* decision, the United States Supreme Court in *Perry v. New Hampshire*[9] reified its outdated standard previously put in place by the Court's opinion in *Manson v. Brathwaite.*[10] In *Manson v. Brathwaite,* the Supreme Court created a test for whether eyewitness identifications were admissible in court.[11] The *Manson* Court held that "reliability is the linchpin in determining the admissibility of identification testimony."[12] Since 1977, when the Court decided *Manson,* decades of research have unfortunately shown how the Court's test misses the mark in enhancing – or securing – reliability of eyewitness identifications. The *Manson* test relies on "the good sense and judgment of American juries."[13] But scholar Elizabeth Loftus' research demonstrates that "[e]yewitness testimony is likely to be believed by jurors,

7. The *Henderson* test established the following steps: (1) the defendant must present evidence of "suggestiveness" to obtain a pretrial hearing; (2) the State then must establish that the identification reliably accounts for both estimator and system variables; (3) the defendant still has the overall burden to show a "substantial likelihood of irreparable misidentification" through either cross-examining eyewitnesses, presenting expert testimony, or by introducing evidence linked with both types of variables; and (4) the court should suppress the identification if it determines, after weighing the evidence, that the defendant demonstrated an irreparable misidentification. *See* State v. Henderson, 27 A.3d 872, 881–82, 920 (N.J. 2011). If the trial court then admits the identification, the court will provide the jury with specific jury instructions at the conclusion of the trial. *Id.* at 924–26; *see also* Amy D. Trenary, State v. Henderson*: A Model for Admitting Eyewitness Identification Testimony*, 84 U. COLO. L. REV. 1257, 1295–96 (2013).

8. *Henderson*, 27 A.3d at 878; *see also* Valena Elizabeth Beety, *Identifying the Culprit in Wrongful Convictions,* 82 TENN. L. REV. 975, 996 (2015) ("The court appointed a Special Master who interviewed seven experts, evaluated the current scientific evidence on eyewitnesses, and then presented the supreme court with 2000 transcript pages and reports on hundreds of scientific studies.").

9. Perry v. New Hampshire, 565 U.S. 228, 248 (2012) ("[T]he Due Process Clause does not require a preliminary judicial inquiry into the reliability of eyewitness identification when the identification was not procured under unnecessarily suggestive circumstances arranged by law enforcement.").

10. 432 U.S. 98, 114 (1977).

11. *Id.*

12. *Id.*

13. *Id.* at 116.

especially when it is offered with a high level of confidence, *even though the accuracy of an eyewitness and the confidence of that witness may not be related to one another at all.*"[14] The *Manson* factors, that is the reliability test created by the Supreme Court, provide little guidance to jurors and are poor indicators of a witness's reliability.[15]

Fast forward to 2012, when the Supreme Court ruled in *Perry v. New Hampshire* that courts did not have to query the reliability of an eyewitness identification before admitting the testimony, unless police held a suggestive pre-trial identification.[16] Justice Sotomayor dissented, quoting *State v. Henderson* that "[t]he empirical evidence demonstrates that eyewitness misidentification is 'the single greatest cause of wrongful convictions in this country.'"[17]

Eyewitness identification is indeed a leading cause of wrongful convictions in DNA exonerations and exonerations more broadly.[18] The concerns about the unreliability of eyewitness identifications led the National Academy of Sciences ("NAS") to investigate. In *Identifying the Culprit: Assessing Eyewitness Identification,* the NAS looked to thirty years of scientific studies and heard presentations from scientists and law enforcement.[19] The National Academy of Sciences recommended that courts (1) conduct pretrial judicial inquiries into eyewitness identifications; (2) admit and present to juries any prior identifications and the confidence levels at the time of the identifications; (3) allow experts to testify on eyewitness memory and identifications; and (4) utilize jury instructions to inform the jury about eyewitness identifications.[20]

Identifying the Culprit criticized the practices for gathering and using eyewitness testimony in a criminal case.[21] The report

---

14. Watkins v. Sowders, 449 U.S. 341, 352 (1981) (Brennan, J., dissenting) (alteration in original) (emphasis added) (quoting ELIZABETH F. LOFTUS, EYEWITNESS TESTIMONY 19 (1979)).

15. *See* Beety, *supra* note 8, at 978. ("The *Manson* test's five factors—the witness's opportunity to view the criminal during the crime, degree of attention, accuracy of prior description, level of certainty, and the length of time between incident and identification—are poor indicators of a witness's reliability.").

16. Perry v. New Hampshire, 565 U.S. 228 (2012).

17. *See id.* at 263 (Sotomayor, J., dissenting) (quoting State v. Henderson, 27 A.3d 872, 885 (N.J. 2011)).

18. *% Exonerations by Contributing Factor*, NAT'L REGISTRY OF EXONERATIONS (Mar. 17, 2022), https://www.law.umich.edu/special/exoneration/Pages/ExonerationsContribFactorsByCrime.aspx.

19. NATIONAL RSCH. COUNCIL OF THE NAT'L ACADS., IDENTIFYING THE CULPRIT: ASSESSING EYEWITNESS IDENTIFICATION 71–102 (2014) [hereinafter IDENTIFYING THE CULPRIT].

20. *Id.* at 109–12.

21. *Id.* at 1–2.

recommends an overhaul of eyewitness identification procedures by police and prosecutors.[22]

Notably, *Identifying the Culprit* was released in 2014, just as police routinely began using facial recognition software.[23] Facial recognition software analyzing stills from surveillance videos allows a third witness to be present, a machine witness – but is that witness reliable?

Recognizing the questionable reliability of eyewitness identifications, facial recognition software may be seen as a good thing, increasing the reliability of identifications in a crime scenario. Yet, just as there are fundamental flaws with eyewitness identification, the same currently holds true for facial recognition software.

II. FACIAL RECOGNITION SOFTWARE

Facial recognition software compares two images and determines whether the same person is present in each image.[24] A probe photo—a still from a surveillance video, for example—can be uploaded to a police database, which includes civilian photos from the Department of Motor Vehicles.[25] The software then compares the probe photo with its database of photos. The software, however, cannot actually "match" two photos. It has fundamental accuracy problems, undermining its reliability.[26] The software provides several possible matches, and a human police officer uses those possible matches as investigative leads.[27]

The use of facial recognition software is not always disclosed to the person ultimately charged with the offense.[28] This failure to disclose can be problematic, given the known inaccuracy of facial recognition software when used to identify people of color.[29]

---

22. *Id.* at 5–7 (such recommendations include, for example, training law enforcement officers in eyewitness identification, implementing double-blind lineups and photo array procedures, standardized witness instructions, and related procedures).

23. *The History of Face Recognition*, FACEFIRST, https://www.facefirst.com/blog/brief-history-of-face-recognition-software/ (last visited Mar. 17, 2022) ("Beginning in 2014, The Automated Regional Justice Information System (ARJIS), began supplying partner agencies with FaceFirst's mobile platform supporting face recognition for law enforcement.").

24. Kaitlin Jackson, *Challenging Facial Recognition Software in Criminal Court,* THE CHAMPION, July 2019, at 14, https://www.nacdl.org/Article/July2019-ChallengingFacialRecognitionSoftwareinCri.

25. *Id.*

26. *Id.*

27. *Id.*

28. *Id.*

29. *Id.* at 15.

III. RACIAL BIAS

Wrongful convictions can be caused by human error, as well as machine error, and both can be influenced by racial bias. Racial bias has been identified as both a cause of faulty human eyewitness identification,[30] as well as faulty facial recognition through software.[31]

Eyewitnesses struggle to identify members of a different racial group, a phenomenon known as "cross-racial misidentification."[32] This phenomenon is particularly harmful against people of color because white people have greater difficulty identifying people of color than vice versa.[33] All people, however, in a famous study where witnesses look at a photograph of a Black man and a white man fighting, were more likely to misremember the Black man as holding the knife.[34] If both men in the photo were white, the witnesses could remember correctly which man was armed. These memory studies show what other research has confirmed: consciously and subconsciously, Americans associated Blackness with crime.[35] This bias can infiltrate itself into technology, which is coded and programed by humans. As Roth notes in *Machine Testimony,* "a machine's programming, whether the result of human coding or machine learning, could cause it to utter a falsehood by design."[36]

Police use of facial recognition software disproportionately affects Black Americans, Asian Americans, and Native Americans.[37] While advocates of technology may claim these systems "do not see

---

30. *See, e.g.*, Radha Natarajan, *Racialized Memory and Reliability: Due Process Applied to Cross-Racial Eyewitness Identifications*, 78 N.Y.U. L. REV. 1821 (2003).

31. *See generally* Ferguson, *supra* note 5, at 1173.

32. Valena Elizabeth Beety, *What the Brain Saw: The Case of Trayvon Martin and the Need for Eyewitness Identification Reform,* 90 DENV. U. L. REV. 331, 341 (2012).

33. John P. Rutledge, *They All Look Alike: The Inaccuracy of Cross-Racial Identifications*, 28 AM. J. CRIM. L. 207, 211 (2001); Christian A. Meissner & John C. Brigham, *Eyewitness Identification: Thirty Years of Investigating the Own-Race Bias in Memory for Faces: A Meta-Analytic Review*, 7 PSYCHOL. PUB. POL'Y & L. 3, 3, 15 (2001).

34. *See* Jennifer L. Eberhardt et al., *Seeing Black: Race, Crime, and Visual Processing*, 87 J. PERSONALITY & SOC. PSYCHOL. 876, 876 (2004) (detailing the 1947 Allport and Postman study).

35. *Id.*

36. Roth, *supra* note 1, at 1977–78. She continues that "[a] machine's output could be imprecise or ambiguous because of human error at the programming, input, or operation stage, or because of machine error due to degradation and environmental forces. And human and machine errors at any of these stages could also lead a machine to misanalyze an event." *Id.* at 1978.

37. Claire Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, CTR. ON PRIV. & TECH. AT GEO. L. (Oct. 18, 2016), https://www.perpetuallineup.org/; *see also* SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM (2018); RUHA BENJAMIN, RACE AFTER TECHNOLOGY: ABOLITIONIST TOOLS FOR THE NEW JIM CODE (2019).

race," research now shows the incorrect identifications of people of color by these programs. Indeed, facial recognition is the least accurate of Black women, even misidentifying their gender.[38]

IV. INFLUENCE OF FACIAL RECOGNITION SOFTWARE ON EYEWITNESS IDENTIFICATION

I wonder, however, about the cascading influence of facial recognition software on eyewitnesses. Police pervasively use facial recognition software and databases.[39] These databases are no longer limited to mug shots; now, nearly half of American adults are in a law enforcement agency's facial recognition network.[40] The Federal Bureau of Investigation routinely runs face recognition searches through their agency's system, and many states allow law enforcement to run searches in driver's license databases or ID photos.[41] These databases include law-abiding citizens.[42] If we combine their wide usage with the lack of accuracy of facial recognition of people of color, and false positives of people of color, we can see how this software can influence eyewitnesses, but also contribute to wrongful convictions if not checked.

Imagine camera footage exists of a crime. Facial recognition software identifies the perpetrator as either Jonathan Jefferson or Clint Alamo, both civilians in the driver's license database. The photos of Jefferson and Alamo are shown to the eyewitness, in a similar manner to a show-up identification. The eyewitness is not instructed that neither may be the culprit, only that the facial recognition software determined one of these was the likely culprit. The influence of this potentially incorrect identification of an individual may be more harmful than a photo show-up, or a photo lineup, because of the added weight given to scientific evidence. Thus, a mistaken facial recognition by software could taint an eyewitness identification, leading to the impression of double confirmation that Jefferson or Alamo is the perpetrator, rather than recognizing how the software finding may have influenced the eyewitness.

Alternatively, if the facial recognition photos are placed in a traditional photo lineup, the safeguards on eyewitness identification –

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

39. Garvie et al., *supra* note 37.

40. *Id.*

41. *Id.*

42. *Id.*

instructions that the culprit may not be present, that it is just as important to exculpate as inculpate people, use of the folder shuffle method to double-blind the use of images – are equally important. Use of a suspect's photo identified by unreliable facial recognition software can also "unreasonably increase[] the chance of eyewitness misidentification."[43]

Yet this is not only a hypothetical. In Spring 2019, police investigating a robbery in Detroit sent a shop surveillance camera image to the Michigan State Police, to match the image to the database of driver's licenses.[44] Facial recognition software identified Robert Williams as the suspect – but Mr. Williams was not the culprit.[45] Still, his driver's license photo was put in a photo lineup and showed to a security consultant for the store who did not witness the robbery itself.[46] Based on the surveillance image and now the driver's license, the consultant incorrectly identified Mr. Williams as the culprit.[47]

Police went to Mr. Williams's home with an arrest warrant and put him in handcuffs in front of his children.[48] They took him to the police station and began interrogating him. Finally, they revealed to Mr. Williams the surveillance photo.[49] A stunned Williams held the photo up to his face and asked the police, "I hope you guys don't think that all Black men look alike."[50] The photo was not Mr. Williams. One police officer sheepishly admitted, "the computer must have gotten it wrong[.]"[51] Unfortunately, the police detained Mr. Williams nearly thirty more hours following this admission.[52]

The potential influence of facial recognition software on eyewitness identification is due to the malleability of human memory. A witness perceives an event, commits that information to memory, and then recalls the memory.[53] But in the final stage of recalling

---

43. *See* Jackson, *supra* note 24, at 17.

44. Man Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart, ACLU (June 24, 2020), https://www.aclu.org/press-releases/man-wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart?msclkid=ec3ffb03bdc411ec85a7795ac4583fd5.

45. *Id.*

46. *Id.*

47. *Id.*

48. *Id.*

49. *Id.*

50. Robert Williams, Opinion, *I Was Wrongfully Arrested Because of Facial Recognition. Why Are Police Allowed to Use It?*,WASH. POST (June 24, 2020), https://www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology/.

51. *Id.*

52. *Id.*

53. *See* LOFTUS, *supra* note 14, at 21.

and reconstructing the event, the memory can be influenced by police protocols, instructions, or feedback. For example, if a witness receives no instructions when shown a lineup of suspects, the witness often assumes the perpetrator of the crime must be in the lineup and is influenced to choose a person.[54] If a witness receives positive feedback from police after making an identification, the feedback increases the witness's confidence in the identification.[55] The eyewitness may give more weight and deference to a software-determined "match" and resulting photo. Research shows that jurors view scientific evidence as particularly reliable and believe that it holds persuasive power.[56] Jurors are inclined to give forensic evidence more weight and value, particularly if an expert witness testifies to it.[57]

V. SOLUTIONS

The solutions that Professor Roth provides in her scholarship are applicable to facial recognition software, and to challenging identifications in court. We can also go upstream to find solutions for an eyewitness influenced by facial recognition software findings.

One upstream solution would be that just as police departments are encouraged to adopt neutralizing procedures for eyewitness identifications, they should implement these procedures for show-ups or line-ups, including facial recognition software findings. The National Academy of Sciences in *Identifying the Culprit* recommended that law enforcement agencies implement protocols such as using double-blind lineup and photo array procedures, developing and using standardized witness instructions, documenting witness statements, and recording the witness identification.[58] The International Association of Chiefs of Police and some state

54. *See* Gary L. Wells et al., *Eyewitness Identification Procedures: Recommendations for Lineups and Photospreads*, 22 LAW & HUM. BEHAV. 603, 625 (1998) ("[E]mpirical data show[s] that eyewitnesses are less likely to identify an innocent suspect when they are warned that the actual culprit might not be present than when they are not so warned.").

55. Amy Bradfield Douglass & Nancy Steblay, *Memory Distortion in Eyewitnesses: A Meta-Analysis of the Post-Identification Feedback Effect*, 20 APP. COGNITIVE PSYCHOL. 859, 865 (2006); Gary L. Wells & Amy L. Bradfield, *"Good, You Identified the Suspect:" Feedback to Eyewitnesses Distorts Their Reports of the Witnessing Experience*, 83 J. APP. PSYCHOL. 360, 361–62 (1998).

56. *See* Valena E. Beety & Jennifer D. Oliva, *Evidence on Fire*, 97 N.C. L. REV. 483, 507 (2019) (citing Valerie P. Hans, *Judges, Juries, and Scientific Evidence*, 16 J.L. & POL'Y 19, 23–24 (2007) (explaining that "jurors themselves have identified the task of interpreting scientific and technical evidence and expert testimony as particularly challenging" and "[c]ase studies examining juror comprehension of scientific testimony, and some experimental research, point out the types of expert evidence that can present problems for juries").

57. *See* Beety & Oliva, *supra* note 56, at 516–17.

58. *See* IDENTIFYING THE CULPRIT, *supra* note 19, at 5.

legislatures adopted the specific police protocols proposed in *Identifying the Culprit.*[59]

The double-blind lineup encouraged for all eyewitness identifications could be particularly effective for identifications reliant on facial recognition software. Creating a double-blind lineup is simple through the Folder Shuffle method.[60] The officer conducting the photo lineup uses manila folders and places a single image in each folder. The officer then randomly shuffles the folders, so the officer does not know which photo is in which folder. Finally, the officer places two empty manila folders at the bottom of the stack, so that the eyewitness does not feel added pressure to pick the last image they see.[61] This process could neutralize any influence that may be present if the eyewitness knew the individual suspect's image came from facial recognition software. The individual so-identified is placed in a photo lineup similar to every other photo in the double blind process. Thus the witness is protected from their own bias, as is the police officer.

Another upstream solution is to apply a more scientific lens to all eyewitness identification evidence.

The National Institute of Standards and Technology ("NIST") has considered creating regular tests for algorithmic bias, and ensuring datasets reflect diversity to diminish racially biased error rates.[62] This follows on a NIST study that evaluated the effects of race, age, and sex on facial recognition software.[63]

NIST also oversees forensic science discipline-specific guidance groups, organized to enhance and ensure quality assurance and quality control.[64] These guidance groups are called Scientific Area

---

59. *National Academy of Sciences Releases Landmark Report on Memory and Eyewitness Identification, Urges Reform of Police Identification Procedures*, INNOCENCE PROJECT (Oct. 2, 2014), http://www.innocenceproject.org/news-events-exonerations/national-academy-of-sciences-releases-landmark-report-on-memory-and-eyewitness-identification-urges-reform-of-police-identification-procedures. *See also Eyewitness Identification Reform*, INNOCENCE PROJECT, https://innocenceproject.org/eyewitness-identification-reform/ (last visited Feb. 5, 2022).

60. *See Groundbreaking Study Finds Double-Blind Sequential Lineups More Accurate in Eyewitness Identifications*, JOHN JAY COLL. CRIM. J. (Sept. 19, 2011), http://johnjay.jjay.cuny.edu/newsroom/4898.php (observing that study participants demonstrated greater errors in simultaneous lineups rather than in sequential lineups, the former of which influence eyewitnesses in identification by providing them a basis for comparison amongst the members of the lineup).

61. For example, Chapter 62 of the West Virginia Code has a detailed description of the folder shuffle method. *See* W.VA. CODE § 62-1E-2.

62. *See* Garvie et al., *supra* note 37.

63. *See NIST Study*, *supra* note 38.

64. *See* ORGANIZATION OF SCIENTIFIC AREA COMMITTEES FOR FORENSIC SCIENCE (OSAC), TERMS OF REFERENCE FOR THE SCIENTIFIC AREA COMMITTEES (2021) (available at

Committees, part of the Organization of Scientific Area Committees. They create standard operating procedures for specified forensic disciplines, while also evaluating research in the field.[65] One Scientific Area Committee ("SAC") is on Digital/Multimedia, including facial recognition and video/imaging technology and analysis.

The use of machines as eyewitnesses will soon necessitate that the Scientific Area Committee that evaluates Facial Identification and Video/Imaging Technology & Analysis also understand and consider the research on eyewitness identification. Within the Digital/Multimedia SAC, I suggest that the subcommittee for Facial Identification consider eyewitness identification, and thus contemplate the impact of facial recognition software on eyewitness identification. Eyewitness identification can be included in the Digital/Multimedia SAC meetings more broadly to focus on quality control and best practices, in line with the extensive research in the field.

This scientific background could further validate experts to testify on eyewitness identification in court, alongside testimony about facial recognition software. By treating eyewitness identification as more scientific, the current divide between human and machine identification can collapse. Parties could present robust data and research in court about the similarities and differences, and the potential influences of one form of identification on the other. Eyewitness identification continues to be used in many courtrooms with no scientifically established standards, and is not understood as related to scientific findings.[66] This could change, for the better.

CONCLUSION AND LOOKING AHEAD

The cascading impact of a faulty machine identification can be seen in Roth's work. This Article has connected the problems of human and machine eyewitness identification, with proposed solutions.

Perhaps in 2032, the biases and problems currently inherent in facial recognition software will be resolved. Perhaps police, prosecutors, and juries will rely more on machine identification rather than human identification. Arguably, that tech will meet the demand in the future. And perhaps this will be a positive move,

---

https://www.nist.gov/system/files/documents/2021/09/13/FSSB_OSAC_ToR%20SAC_v2.2.pdf). *See also* Beety, *supra* note 8, at 985.

65. *OSAC Subcommittees*, NAT'L INST. OF STANDARDS & TECH. (Nov. 5, 2021), https://www.nist.gov/osac/osac-subcommittees.

66. *See* Beety, *supra* note 8, at 990–91.

though it is questionable how much we as a society wish to rely on surveillance for evidentiary needs.

But just as we currently have technology deserts and rural communities without broadband – indeed, states where nearly fifty percent of the population does not have internet access – I anticipate machine identification will still not be a reliable resource in rural and underserved areas. We will still be relying on eyewitness identifications. And to that end, it is important to have an OSAC that considers eyewitness identification as scientific evidence, and that courts seek greater reliability in this field.

By recognizing the connections between machine and human identifications, we can work to enhance the reliability of both. We have structures in place to heighten the scientific reliability of machine identifications, and proposals for law enforcement to increase the accuracy of human identifications. Working together, we can increase accuracy in the courtroom, and prevent wrongful convictions due to misidentifications.