FACING THE FUTURE: FACIAL RECOGNITION TECHNOLOGY UNDER THE CONFRONTATION CLAUSE

Emma Lux*

INTRODUCTION

In 2015, two undercover police officers purchased cocaine from an African American individual and snapped several photographs of his face.[1] Unable to identify the individual's name, police sent the photograph to an analyst who used a facial recognition program to determine whether the face looked like any mugshots in the county database.[2] The algorithm returned Willie Lynch's face as a match, but indicated "only *one star* of confidence" that the match was correct.[3]

The prosecutor in Lynch's case did not seek to introduce the facial recognition results at trial, instead relying on in-court identifications by the officers.[4] However, the day where prosecutors seek admission of facial recognition evidence to identify criminal defendants at trial is growing closer.[5] What happens when a prosecutor wants to tell a jury that a facial recognition algorithm matched Willie Lynch to the image of the perpetrator?

This piece imagines what that day will look like. Part I begins with a brief overview of facial recognition technology to inform the discussion that follows. Part II analyzes facial recognition evidence under *Melendez-Diaz v. Massachusetts*[6] and *Bullcoming v. New Mexico*,[7] arguing that the evidence is testimonial hearsay and therefore subject to confrontation. Part III then provides practical advice for defense attorneys who may need to cross-examine a facial recognition analyst in the near future.

---

* Emma Lux is a *juris doctor* candidate at the Georgetown University Law Center, with expected graduation in 2021. She is a Featured Online Contributor for Volume 57 of the *American Criminal Law Review*.

[1] Somil Trivedi & Nathan Freed Wessler, *Florida Is Using Facial Recognition to Convict People Without Giving Them a Chance to Challenge the Tech*, ACLU (Mar. 12, 2019, 5:15 PM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/florida-using-facial-recognition-convict-people.

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *See* John Nawara, *Machine Learning: Face Recognition Technology Evidence in Criminal Trials*, 49 U. LOUISVILLE L. REV. 601, 609–18 (arguing that facial recognition technology currently "passes muster under both Frye and Daubert").

[6] Melendez-Diaz v. Massachusetts, 557 U.S. 305 (2009).

[7] Bullcoming v. New Mexico, 564 U.S. 647 (2011).

I. AN OVERVIEW OF FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology is a type of machine learning technology.[8] Before machine learning technology, computers used to operate solely by command[9]—that is, a programmer would enter a command, and the computer would perform that command.[10] But with facial recognition technology, a technician need not program the precise commands necessary for the machine to determine that a face matches another face.[11] Rather, the machine "learns" over time how to identify whether one particular face looks like another.[12] The "learning" happens through "probe photographs," where a coder shows the machine a face, allows the machine to estimate whether or not the probe image matches any faces in its database, and then informs the machine whether its final result was right or wrong.[13] After thousands of iterations, the machine "learns" to identify whether a probe photograph looks like another face and reduces its error rate with each repetition.[14]

Such a brief description of how the technology works, however, creates a false illusion of a computer autonomously generating results.[15] As demonstrated below, this false assumption threatens to undermine a criminal defendant's right to confront the analyst who prepared a facial recognition report under the Confrontation Clause.[16] Thus, defense attorneys should understand three critical aspects of facial recognition technology in order to argue that such evidence is testimonial.[17]

First, contrary to popular belief, facial recognition technology does not actually report that a face "matches" a face in its database

---

[8] Nawara, *supra* note 5, at 601.

[9] *See* Christian Chessman, *A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 CAL. L. REV. 179, 181 (2017) ("A computer program is nothing more than an organized series of commands given by a human computer programmer.").

[10] *Id.*

[11] Nawara, *supra* note 5, at 601 (explaining that "a [facial recognition] program learns to recognize faces after being shown millions of sample faces").

[12] *Id.*

[13] Oliver Tan, *How Does A Machine Learn?*, FORBES (May 2, 2017, 7:00 AM), https://www.forbes.com/sites/forbestechcouncil/2017/05/02/how-does-a-machine-learn/#31f614e97441.

[14] *Transparency Note: Azure Cognitive Services Face API*, MICROSOFT 1, 5 (Mar. 29, 2019), https://azure.microsoft.com/mediahandler/files/resourcefiles/transparency-note-azure-cognitive-services-face-api/Face%20API%20Transparency%20Note%20(March%202019).pdf? [hereinafter *Transparency Note*].

[15] Joseph Clarke Celentino, *Face-To-Face with Facial Recognition Evidence: Admissibility under the Post-Crawford Confrontation Clause*, 114 MICH. L. REV. 1317, 1342 (2016) (explaining that, though facial recognition evidence operates behind a "scrim of automation," the "inputs of actual people" influence the results).

[16] *See infra* Section II.

[17] Crawford v. Washington, 541 U.S. 36, 53–54 (2004).

autonomously.[18] Rather, the machine automatically reports the *probability* that a particular probe photograph, the image inputted for analysis, matches a database image.[19] The computer produces a number ranging from 0 to 1, called a "match score," and "describes the similarity between [the probe] image and an [image in the database]."[20] The higher a match score, the "more likely [it is] that the two images are the same person."[21]

For a facial recognition algorithm to report a "match," a human must manually enter a confidence threshold into the machine.[22] The confidence threshold is "a configurable value between 0 to 1 that determines the match score required to be considered a positive match."[23] Selecting a confidence threshold requires skill and judgment by the programmer,[24] and lowering the threshold affects the reliability and accuracy of the results.[25] For example, Amazon has stated that its facial recognition software, Rekognition, only reports reliable matches for human faces at a confidence threshold of 99 percent or more.[26]

In the criminal context, however, law enforcement agencies that purchase facial recognition software from third-parties[27] often have the ability to manipulate the confidence threshold despite the recommendations of the manufacturer.[28] The Washington County Sheriff's Office in Oregon, for example, employed Amazon's Rekognition software to identify a suspect at a 96.03 confidence

---

[18] Celentino, *supra* note 15, at 1342.
[19] *Transparency Note, supra* note 14, at 5.
[20] *Id.*
[21] *Id.*
[22] *See id.* at 5–6 (describing how to choose a confidence threshold).
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] Jake Laperruque, "*About-Face: Examining Amazon's Shifting Story on Facial Recognition Accuracy*," PROJECT ON GOVERNMENT OVERSIGHT (April 10, 2019), https://www.pogo.org/analysis/2019/04/about-face-examining-amazon-shifting-story-on-facial-recognition-accuracy/ (noting that Amazon originally recommended a 95 percent confidence threshold, before increasing the threshold following criticism from civil rights organizations).
[27] Amazon is a "major vendor [of facial recognition technology] to law enforcement." *Id.* Other companies that provide facial recognition technology to law enforcement include Cognitec and Vigilant Solutions. Clare Garvie, *Garbage In, Garbage Out*, GEORGETOWN LAW: CENTER ON PRIVACY AND TECHNOLOGY (May 16, 2019), https://www.flawedfacedata.com.
[28] *See, e.g.*, *Use Cases That Involve Public Safety*, AMAZON REKOGNITION DEVELOPER GUIDE (last visited Jan. 4, 2020), https://docs.aws.amazon.com/rekognition/latest/dg/considerations-public-safety-use-cases.html (explaining how law enforcement can use the software below the recommended confidence threshold "for scenarios that benefit from a larger set of potential matches").

threshold,[29] below the 99 percent threshold that Amazon recommends "to ensure that a person's civil rights are not violated."[30]

Second, attorneys should be aware that the accuracy of facial recognition technology depends on the probe photograph's characteristics.[31] Facial recognition technology is less accurate when probe photographs are "pixelated, distorted, or of partial faces," which is often the case for surveillance images.[32] The technology is also less reliable when police alter probe images so the computer "can interpret [them] more easily,"[33] a practice police have utilized.[34] For example, police have "mirror[ed]"a partial face to approximate the features on the other side of the face;[35] removed facial expressions, such as replacing an open mouth with a closed one;[36] and, in one bizarre instance, replaced a blurry surveillance camera image with a photograph of Woody Harrelson.[37] Lastly, probe photographs are less likely to produce a credible match when they depict African American or female suspects.[38] This means that both women and African Americans "will disproportionately bear the harms of face recognition misidentification"[39] not only at trial, but also during police investigations where facial recognition technology is often used to identify suspects.[40]

Third, the practical realities and incentives of the facial recognition industry are relevant to the Confrontation Clause analysis. The Court has

---

[29] Bryan Menegus, *Defense of Amazon's Face Recognition Tool Undermined by Its Only Known Police Client*, GIZMODO (Jan. 31, 2019, 4:55 PM), https://gizmodo.com/defense-of-amazons-face-recognition-tool-undermined-by-1832238149.

[30] *Use Cases That Involve Public Safety*, *supra* note 28.

[31] Garvie, *supra* note 27 (describing how flawed data entered into a facial recognition algorithm can affect the accuracy of the results).

[32] *Id.*

[33] Nawara, *supra* note 5, at 609.

[34] Garvie, *supra* note 27.

[35] *Id.*

[36] *Id.*

[37] *Id.* (discussing how police altered the image since a detective conducting the facial recognition program thought that "the suspect looked like the celebrity").

[38] Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, WIRED (July 22, 2019, 7:00 AM), https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/ (explaining that top-performing facial recognition systems still misidentify African Americans at rates five to ten times higher than whites, and are also less accurate at identifying women than men).

[39] Clare Garvie & Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, GEORGETOWN LAW: CENTER ON PRIVACY AND TECHNOLOGY (May 16, 2019), https://www.americaunderwatch.com/ (describing how "the technology still exhibits race and gender bias").

[40] Kaitlin Jackson, *Challenging Facial Recognition Software in Criminal Court*, 43 CHAMPION 14, 14 (Jul. 2019) (describing how police have used facial recognition technology to investigate crimes such as drug sales, petty theft, and identity theft).

contemplated the risk of fraud[41] and error[42] for particular forensic sciences when determining whether a statement is testimonial. The first time the Court found a forensic laboratory report to be testimonial,[43] for example, it reasoned that confrontation was necessary in part because forensic scientists, who often rely on law enforcement for employment, may feel "pressure to sacrifice appropriate methodology for the sake of expediency."[44] Thus, it is relevant to the testimonial analysis that data about police use of facial recognition is often shrouded in secrecy,[45] that police have utilized confidence thresholds below recommended levels,[46] and that third-party companies have "obfuscated" the risks of the technology in order to continue benefiting from law enforcement's business.[47]

The discussion that follows informs defense attorneys about how the above characteristics weigh on the Confrontation Clause analysis and provide ammunition for cross-examining facial recognition analysts.

II. FACIAL RECOGNITION TECHNOLOGY AND THE CONFRONTATION CLAUSE

The Confrontation Clause generally bars admission of testimonial hearsay from a witness who does not appear at trial, unless the witness was unavailable to testify and the defendant previously had an opportunity for cross-examination.[48]

A. *The Primary Purpose Test*

To trigger the Confrontation Clause, a statement must be testimonial.[49] A statement is testimonial when it has the primary purpose of "'establish[ing] or prov[ing] past events potentially relevant to later

---

[41] *See, e.g.*, Williams v. Illinois, 567 U.S. 50, 85–86 (2012) (reasoning that a statement was not testimonial in part because there was no real risk of fraud when forensic testing produced only an anonymous DNA profile).

[42] *See, e.g.*, *id.* at 118–19 (2012) (Kagan, J., dissenting) (describing how the Confrontation Clause is the constitutional "mechanism for catching…errors [in forensic analysis]," such as when an analyst realized that she had accidentally switched two DNA samples during cross-examination).

[43] Melendez-Diaz v. Massachusetts, 557 U.S. 305 (2009).

[44] *Id.* at 318 (quoting COMMITTEE ON IDENTIFYING THE NEEDS OF THE FORENSIC SCIENCES COMMUNITY, *Strengthening Forensic Science in the United States: A Path Forward*, National Academy of Sciences (2009) https://www.ncjrs.gov/pdffiles1/nij/grants/228091.pdf). *See also* George Fisher, EVIDENCE 883–84 (Robert C. Clark et al. eds., 3d ed. 2013).

[45] Trivedi & Wessler, *supra* note 1.

[46] Menegus, *supra* note 29.

[47] *See* Laperruque, *supra* note 26 (explaining how Amazon, who partners with police to provide facial recognition, has defended law enforcement's use of low confidence thresholds to the media).

[48] Celentino, *supra* note 15, at 1333.

[49] Whorton v. Bockting, 549 U.S. 406, 418 (2007).

criminal prosecution'"[50] and is offered for "purposes [of] establishing the truth of the matter asserted."[51] As demonstrated below, facial recognition evidence will likely satisfy the primary purpose test as set forth in *Bullcoming v. New Mexico*.[52]

The Supreme Court has never reached a majority regarding a precise definition of the "primary purpose" test. In *Bullcoming v. New Mexico*, a four-justice plurality wrote that a statement must have the "primary purpose" of "establish[ing] or prov[ing] past events potentially relevant to later criminal prosecution."[53] For example, a statement made to establish the defendant's blood alcohol level before trial satisfied the test,[54] but a statement made with the "primary purpose of . . . enabl[ing] police assistance to meet an ongoing emergency" did not.[55] Thus, a domestic abuse victim's statements to a 911 operator while the defendant was allegedly in her home were not testimonial.[56]

Reports containing the results of a forensic analysis also trigger the Confrontation Clause if they are testimonial in nature.[57] In *Melendez-Diaz v. Massachusetts*, the prosecution introduced the results of a forensic report identifying a seized substance as cocaine.[58] The defendant argued that his inability to cross-examine the analyst who created the report violated the Confrontation Clause.[59] The Court agreed, holding that the

---

[50] Bullcoming v. New Mexico, 564 U.S. 647, 659 n.6 (2011) (quoting Davis v. Washington, 547 U.S. 813, 822 (2006)). It remains an open question *whose* primary purpose is the proper measure. The late Justice Scalia and Justice Sotomayor disagreed over whether the primary purpose test is objective or subjective in *Michigan v. Bryant*. Michigan v. Bryant, 562 U.S. 344, 360 (2011) (holding that "[t]he relevant inquiry is . . . the purpose that reasonable participants would have had, as ascertained" from the circumstances, in an opinion authored by Justice Sotomayor); *but see Bryant*, 562 U.S. at 381 (Scalia, J., dissenting) ("[T] he declarant must intend the statement to be a solemn declaration . . . and he must make the statement with the understanding that it may be used to invoke the coercive machinery of the State against the accused.").

[51] Crawford v. Washington, 541 U.S. 36, 59 n.9 (2004).

[52] *Bullcoming*, 564 U.S. at 659 n.6 (quoting Davis v. Washington, 547 U.S. 813, 822 (2006).

[53] *Id.* The Court has also held that a testimonial statement is a "solemn declaration[] . . . made for the purpose of proving some fact." Crawford v. Washington, 541 U.S. 36, 51 (2004). Testimonial statements do not include casual remarks made to an acquaintance; *id.* at 51; or statements made in furtherance of a conspiracy. *Id.* at 56. This piece does not contemplate Justice Thomas's view on what evidence is testimonial, since no other Justice joins in his view. *See* Williams v. Illinois, 567 U.S. 50, 141 (2012) (Kagan, J., dissenting) (describing Justice Thomas's "one-justice view of [*Melendez-Diaz* and *Bullcoming*]").

[54] *Bullcoming*, 564 U.S. at 658.

[55] Davis v. Washington, 547 U.S. 813, 822 (2006).

[56] *Id.* at 828.

[57] Melendez-Diaz v. Massachusetts, 557 U.S. 305, 310 (2009) (quoting Crawford v. Washington, 541 U.S. 36, 51 (2004)) (explaining that the forensic lab reports indicating the presence of cocaine fell "within the 'core class of testimonial statements'" with which the Confrontation Clause is concerned).

[58] *Id.* at 309.

[59] *Id.* at 310.

report was a testimonial statement.[60] The report satisfied the primary purpose test because its sole purpose under Massachusetts law was to provide evidence against the defendant, and the report was "prepared specifically for use at [the defendant's] trial."[61] Additionally, the majority reasoned that the statements were testimonial because the report did "precisely what a witness does on direct examination."[62]

But in *Williams v. Illinois*, the Court's most recent forensic reports case, the Court held that a DNA forensic report, when discussed by an expert but not introduced into evidence, did not constitute testimonial evidence subject to confrontation.[63] There, the plurality, written by Justice Alito, applied a narrower "primary purpose" test than in *Bullcoming*.[64] The plurality found that the report was not testimonial because it was not "prepared for the primary purpose of accusing a targeted individual" who was in custody or under investigation.[65] Rather, the Court found that the report's primary purpose "was to catch a dangerous rapist who was still at large" because the defendant was neither under investigation or in custody at the time of the test.[66] Additionally, confrontation was not necessary, the plurality reasoned, since the lab technicians did not know that their testing would inculpate the defendant,[67] and the DNA testing produced only an anonymous DNA profile, reducing fraudulent incentives.[68]

Under the narrower *Williams* plurality rule, which has tenuous precedential value,[69] the testimonial nature of facial recognition evidence will depend on the circumstances. When police use the technology to identify people already in police custody, the technology would satisfy the *Williams* plurality's primary purpose test since the technology would

---

[60] *Id.* at 324.
[61] *Id.*
[62] *Id.* at 310–11 (quoting *Davis*, 547 U.S. at 813). *See also Crawford*, 541 U.S. at 51 (describing how testimonial statements include "*ex parte* in-court testimony or its functional equivalent").
[63] Williams v. Illinois, 567 U.S. 50, 58 (2012). The five-justice majority was formed by Justice Alito's plurality and Justice Thomas, who concurred in the judgment, but explicitly rejected the plurality's reasoning. *Id.* at 103 (Thomas, J., dissenting).
[64] *Id.* at 84 (stating that a statement must be "prepared for the primary purpose of accusing a targeted individual" to be testimonial). *C.f.* Bullcoming v. New Mexico, 564 U.S. 647, 659 n.6 (2011) (stating that a statement is testimonial when it "ha[s] the 'primary purpose' of 'establish[ing] or prov[ing] past events potentially relevant to later criminal prosecution'") (quoting Davis v. Washington, 547 U.S. 813, 822 (2006)).
[65] *Id.*
[66] *Id. C.f. Melendez-Diaz*, 557 U.S. 305, 307 (2009) (explaining how the defendant was already under investigation when the police submitted his sample for forensic analysis).
[67] *Williams*, 567 U.S. 50 at 85.
[68] *Id.* at 85–86.
[69] *See, e.g.*, State v. Dotson, 450 S.W. 3d 1, 68 (Tenn. 2014) ("The Supreme Court's fractured decision in *Williams* provides little guidance and is of uncertain precedential value"); State v. Michaels, 95 A.3d 648, 666 (N.J. 2014) ("We find *Williams*'s force, as precedent, at best unclear.").

be used to "obtain evidence for use against" the particular defendant.[70] However, police have also used facial recognition technology to find unidentified perpetrators of serious crimes like shootings.[71] Those situations are more akin to "ongoing emergenc[ies]" which would not be testimonial under the *Williams* plurality reasoning, but only four justices, including Justice Kennedy, endorsed the *Williams* reasoning.[72] Additionally, facial recognition evidence is distinguishable from DNA evidence under *Williams*.[73] Facial recognition technicians are more likely than DNA technicians to know that their testing will inculpate a defendant,[74] since surveillance probe images typically show people committing crimes.[75] Additionally, facial recognition technology is less reliable than DNA evidence[76] and does not produce anonymous results, which increases fraudulent incentives.[77]

Under *Melendez-Diaz* and *Bullcoming*, by contrast, facial recognition technology will likely satisfy the primary purpose test, even when police are investigating an unidentified individual. Recall that the more lenient interpretation requires only "establish[ing] or prov[ing]" that "past events" are "potentially relevant to later criminal prosecution."[78] Using that analysis, even if a particular defendant has yet to be identified, facial recognition results would undoubtedly be used to "prove past events *potentially* relevant to later criminal prosecution."[79] Additionally, tracking the reasoning of *Melendez-Diaz*, a facial recognition match really is the "functiona[l]" equivalent of "in-court testimony, doing

---

[70] *Williams*, 567 U.S. 50 at 84.

[71] *See, e.g.*, Derek Hawkins, *How Maryland Police Used Facial Recognition to Catch Annapolis Shooter Jarrod Ramos*, THE INDEPENDENT (July 2, 2018, 8:11 PM), https://www.independent.co.uk/news/world/americas/annapolis-shooting-maryland-police-facial-recognition-catch-jarrod-ramos-a8427181.html.

[72] *See Williams*, 657 U.S. 50 at 55 (reasoning that the statement was nontestimonial because it was made during an "ongoing emergency").

[73] *Id.* at 85.

[74] *Id.* at 85 ("When lab technicians are asked to work on the production of a DNA profile, they often have no idea what the consequences of their work will be.").

[75] *See, e.g.*, Trivedi & Wessler, *supra* note 1 (describing how a photograph taken by undercover police of a man selling illegal drugs was analyzed with facial recognition technology); *c.f. Williams*, 657 U.S. 50 at 85 (distinguishing the *Williams* nontestimonial DNA test from the laboratory reports in *Melendez-Diaz* and *Bullcoming*, in which "the technicians who prepared the reports must have realized that their contents [which reported an elevated blood-alcohol level and the presence of an illegal drug] would be incriminating").

[76] Garvie, *supra* note 27 (describing how facial recognition results are easily manipulated by input procedures of technicians); *c.f. Williams*, 657 U.S. 50 at 85 (noting that "there is no real chance" of fraud for DNA samples due to the number of parties involved).

[77] Celentino, *supra* note 15, at 1349 (describing how facial recognition analysts may be tempted to fraudulently alter the returned results, for example, if a "photo depicts the analyst's mother committing a crime"); *c.f. Williams*, 657 U.S. at 85 (noting that DNA laboratory results are anonymous).

[78] Bullcoming v. New Mexico, 564 U.S. 647, 659 n.6 (2011) (quoting Davis v. Washington, 547 U.S. 813, 822 (2006)).

[79] *Id.*

'precisely what a witness does on direct examination.'"[80] Just as the *Melendez-Diaz* affidavit attested to the presence of cocaine in the defendant's system—"the precise testimony the analysts would be expected to provide if called at trial"[81]—facial recognition technology would similarly attest to the presence of a defendant in a video or image of a person perpetrating a crime.[82]

B. *Computerized Evidence and Hearsay*

In addition to satisfying the primary purpose test, a statement must constitute hearsay to be testimonial.[83] Hearsay is a "statement" that "the declarant does not make while testifying at the current trial or hearing" and is "offer[ed] [into] evidence to prove the truth of the matter asserted in the statement."[84] Because a "statement" is defined as a "person's . . . assertion,"[85] the main question in the context of computerized facial recognition and forensic reports is whether the "statement" that the machine produces contains sufficient human involvement to constitute hearsay, a question the Supreme Court has not yet addressed.[86]

Almost all federal courts have admitted computer records into evidence under hearsay exceptions, implicitly finding that the evidence is

---

[80] Melendez-Diaz v. Massachusetts, 557 U.S. 305, 310–11 (2009).
[81] *Id.* at 310.
[82] Trivedi & Wessler, *supra* note 1 ("If the witness testified that she was 'one-star confident' that [a defendant] was the drug seller, wouldn't you want to know if she had thought any other individuals, besides [the defendant], were equally likely to be the guy?").
[83] Crawford v. Washington, 541 U.S. 36, 59 n.9 (2004) (holding that the Confrontation Clause "does not bar the use of testimonial statements for purposes other than establishing the truth of the matter asserted"); *c.f.* FED. R. EV. 801(c)(2) (defining hearsay, *inter alia*, as a statement "offer[ed] in evidence to prove the truth of the matter asserted in the statement"). *See also* Poorbaugh, *Interfacing Your Accuser: Computerized Evidence and the Confrontation Clause Following Melendez-Diaz*, 23 REGENT UNIV. L. REV. 213, 221 (2011) (noting that computerized evidence must be a statement made by a person to trigger the Confrontation Clause since the "the notion of a machine itself taking the witness stand for cross-examination approaches the realm of science fiction"); *c.f.* FED. R. EV. 801(a) (requiring that a person makes a statement for the statement to constitute hearsay).
[84] FED. R. EV. 801(c). In *Williams v. Illinois*, Justice Alito's plurality reasoning left open the possibility that a DNA laboratory report is not offered for a hearsay purpose when an expert relies on that report to form their opinion, but the report itself is not admitted. 567 U.S. 50, 77–78 (2012). How the *Williams* plurality's hearsay analysis applies to facial recognition evidence is outside the scope of this article. However, though Justice Gorsuch has not yet participated in deciding a Confrontation Clause laboratory reports case, he recently indicated that he does not support the reasoning of the *Williams* plurality in an opinion dissenting from the denial of certiorari in Stuart v. Alabama, 139 S.Ct. 36 (2018) (Gorsuch, J., dissenting).
[85] FED. R. EV. 801(a).
[86] Adam Wolfson, *Electronic Fingerprints: Doing Away with the Conception of Computer-Generated Records as Hearsay*, 104 MICH. L. REV. 151, 155 (2005).

a hearsay statement made by a person.[87] A minority of courts have explicitly addressed whether there is a distinction between "computer-generated" and "computer-stored" evidence, holding that only the latter is hearsay potentially subject to confrontation.[88] For example, an IRS report that was based on data "made and preserved" by public officials[89] would constitute computer-stored evidence "entered by a human" and would be subject to confrontation if the statements were also testimonial.[90]

By contrast, "computer-generated" forensic reports, courts have reasoned, "involv[e] so little intervention by humans in [their] generation" that the reports do not constitute hearsay subject to the Confrontation Clause.[91] For example, a "header" that appeared when a defendant uploaded information to the internet, which included the "screen name, subject of the posting, date of the posting, and the [uploading individual's] IP address" was not hearsay since it "was generated instantaneously without the assistance or input of a person."[92] The moment that the defendant uploaded the images, the computer produced the defendant's identifying information.[93]

In theory, the minority approach makes sense, and commentators have advocated for it.[94] The problem arises when courts attempt to apply this "computer-stored" versus "computer-generated" distinction[95] to technologies they do not understand well, using incorrect assumptions about the mechanical, neutral nature of computers.[96] *United States v. Washington* is illustrative.[97] There, the majority held that the raw data generated by a blood alcohol machine was computer-generated, not a statement of the technicians who operated the machine, and thus the defendant was not entitled to confront the technicians in court.[98] The opinion ignored the fact that the blood alcohol machine literally could not have produced a conclusion absent human input, namely the entry of the

---

[87] *Id. See, e.g.*, United HealthCare Corp. v. Amer. Trade Ins. Co., 88 F.3d 563, 574 n.7 (8th Cir. 1996) (assuming that an individual's computer forms constituted hearsay admissible under the business records exception to the hearsay rule); Potamkin Cadillac Corp. v. B.R.I. Coverage Corp., 38 F.3d 627, 632 (2d Cir. 1994) ("A business record may include data stored electronically on computers.").
[88] Wolfson, *supra* note 86, at 157–158.
[89] *See, e.g.*, United States v. Neff, 615 F.2d 1235, 1241 (9th Cir. 1980).
[90] Poorbaugh, *supra* note 83, at 222.
[91] United States v. Lamons, 532 F.3d 1251, 1263 n.23 (2008).
[92] United States v. Hamilton, 413 F.3d 1138, 1142 (2005).
[93] *Id.*
[94] Wolfson, *supra* note 86, at 158.
[95] *Id.* at 157–158.
[96] Curtis E.A. Karnow, *The Opinion of Machines*, COLUM. SCI. AND TECH. L. REV. 136, 139 ("Many judges do not have [the] knowledge [to handle the technical issues]"). *See also* Chessman, *supra* note 9, at 184, n.25 ("[Computers'] appearance of autonomy often bolsters the assumption that computer programs are independent, objective, or free of human biases.").
[97] United States v. Washington, 498 F.3d 225 (4th Cir. 2007).
[98] *Id.* at 231.

sample into the machine.[99] Thus, any "results" the machine produced were necessarily informed by any errors or fraud committed by the human entering that information into the machine.[100]

There is a high risk that courts will similarly misapply the computer-generated versus computer-stored distinction to facial recognition technology. Recall from the above[101] that facial recognition technology is a type of machine learning, which at first glance appears to act autonomously.[102] Thus, courts may be tempted to classify reports from facial recognition programs as computer-generated, not subject to confrontation.[103]

When faced with courts that are skeptical of the human effect on facial recognition output, defense attorneys should point out that facial recognition technicians can significantly alter the accuracy of the output.[104] This makes the technology more like the IRS report,[105] subject to human error, than the computer that produced the identifying headers automatically.[106] Because the accuracy of a facial recognition report depends on the confidence threshold selected by the technician,[107] the quality of the probe photograph,[108] if and how it has been altered,[109] and whether it features an African American person or a woman,[110] there are many steps in which evidence can be manipulated or mishandled. Additionally, it is relevant to the Confrontation analysis[111] that those selecting the confidence threshold—law enforcement agencies—have already been found to utilize techniques that reduce the reliability of results.[112]

---

[99] *Id.* (Michael, J., dissenting) (arguing that "[i]n light of the significant role that the technician plays in conducting the test and generating accurate results, the results" constitute hearsay).

[100] *See* Williams v. Illinois, 567 U.S. 50, 118–19 (2012) (Kagan, J., dissenting) (describing how an analyst accidentally switched two DNA samples, thus producing an incorrect result).

[101] *See supra* Section I.

[102] Celentino, *supra* note 15, at 1342.

[103] United States v. Washington, 498 F.3d 225, 231 (4th Cir. 2007).

[104] Celentino, *supra* note 15, at 1342.

[105] United States v. Duncan, 30 M.J. 1284, 1289 (1990).

[106] United States v. Hamilton, 413 F.3d 1138, 1142 (2005).

[107] *Transparency Note*, *supra* note 14.

[108] Garvie, *supra* note 27.

[109] *Id.*

[110] Simonite, *supra* note 38.

[111] *See* Melendez-Diaz v. Massachusetts, 557 U.S. 305, 318 (2009); *see also* Williams v. Illinois, 567 U.S. 50, 85–86 (2012).

[112] Menegus, *supra* note 29 (describing how police have utilized confidence thresholds below the suggested percentage); Garvie, *supra* note 27 (describing how police have altered probe photographs).

III. HOW TO CHALLENGE FACIAL RECOGNITION EVIDENCE

Assume that a court navigates all of this correctly, and properly determines that a defendant may challenge the technology. Now what? What should a defense attorney highlight? The analysis is fact-specific, and different facial recognition technologies will require different cross-examinations. However, as described above,[113] there are three main elements of facial recognition technology that pose the greatest risk of error, and thus the defense attorney should aim to highlight at least these three elements while confronting the facial recognition technician.

Perhaps the most important thing to do is bust the myth that machine learning is autonomous.[114] Courts carry assumptions[115] about the autonomy of computers that threaten to cause them to misapply Confrontation Clause doctrine to facial recognition technology. As a result, defense attorneys should first point out any discrepancy between the threshold recommended by the technology's manufacturer and the confidence threshold that law enforcement applied.[116] By providing the benchmark of the recommended threshold, the attorney can demonstrate how human choices influence the reliability of the results, and give the factfinder a marker by which to measure the credibility of the current threshold level.

Second, since there is also significant potential for altering the accuracy of the results during the probe photograph input,[117] the defense attorney should inquire into the state of the probe photograph and the process by which it was inputted into the program. Namely, facial recognition technology is less accurate when probe images are "pixelated, distorted, or of partial faces."[118] The technology is also less reliable when the analyst has altered the probe images to make them more machine-readable,[119] or when the probe photograph features an African American person or a woman.[120] The defense attorney should thus seek to identify the quality of the probe photograph, and whether it was altered in any way,[121] from the facial recognition analyst under cross-examination.

---

[113] *See supra* Section I.

[114] *See Transparency Note*, *supra* note 14, at 5–6 (describing the human input in deciding whether a face constitutes a match).

[115] Chessman, *supra* note 9, at 184, n.25 ("[Computers'] appearance of autonomy often bolsters the assumption that computer programs are independent, objective, or free of human biases.").

[116] *See* Laperruque, *supra* note 26 (describing a police department's use of a 96.03 percent confidence threshold when the manufacturer recommended at least 99 percent).

[117] Garvie, *supra* note 27.

[118] *Id.*

[119] *Id.*

[120] Simonite, *supra* note 38.

[121] Whether the facial recognition analyst altered the probe image is also relevant so that the jury can assess the credibility of the confidence threshold. Recall that altered images not only lower the likelihood that the match is correct, but also potentially warp the confidence level of the machine if its confidence derives from the altered portions rather

Furthermore, pointing out the risk of fraud and error among current facial recognition technologists is worthwhile, at the very least to emphasize to the court the drastic effects that human error can have on facial recognition analysis and assist the court in its hearsay analysis.[122] Notably, though the admissibility of expert testimony is outside the scope of this piece, pointing out the risk of fraud and error inherent to facial recognition technology may also be helpful in that context. Even if courts admit the facial recognition expert's testimony, they are more likely to require that the expert couch evidence in careful terms and not overemphasize the credibility of the results.[123] Thus, a court would at least restrict an expert from overemphasizing the significance of a match.[124]

CONCLUSION

The very thing that threatens to bias juries—the reporting of a "match"—is the very aspect of facial recognition technology that humans have the most control over.[125] Confidence thresholds can be manipulated to report "matches" at lower levels, which has the potential to mislead a jury by exaggerating the credibility of the results.[126] Furthermore, human manipulation, and thus possibilities for error, are present throughout the process, including at the initial stage in which the analyst inputs the probe photograph and potentially alters it.[127] The human input necessarily makes facial recognition reports hearsay, and the context in which such reports are produced would almost always result in testimonial statements with the primary purpose of "establish[ing] or prov[ing] past events potentially relevant to later criminal prosecution."[128] As the ACLU sensibly put it, "[i]f [a] witness testified that she was 'one-star confident' that [a defendant] was the [perpetrator], wouldn't you want to know . . . what exactly she meant by 'one-star confident?'"[129] That scenario is getting closer,[130] and the Confrontation Clause remains the best

---

than the probe photograph. *Id.* ("This means that the original photo could represent 60 percent of a suspect's face, and yet the algorithm could return a possible match assigned a 95 percent confidence rating, suggesting a high probability of a match to the detective running the search.").

[122] *See* Williams v. Illinois, 567 U.S. 50, 118–19 (2012) (Kagan, J., dissenting) (describing how the Confrontation Clause is the constitutional "mechanism for catching…errors [in forensic analysis]").

[123] GEORGE FISHER, EVIDENCE 883–84 (Robert C. Clark et al. eds., 3d ed. 2013) (describing how courts, in response to emerging evidence that forensic reports are unreliable, often require experts to state their conclusions in careful terms so as not to mislead the jury as to the test's reliability).

[124] *Id.* (describing how the National Academy of Sciences previously criticized forensic fingerprint analysts for reporting a "match" on the basis of "uncertain data").

[125] *Transparency Note*, *supra* note 14, at 56.

[126] *Id.*

[127] Garvie, *supra* note 27.

[128] Davis v. Washington, 547 U.S. 813, 822 (2006).

[129] Trivedi & Wessler, *supra* note 1.

[130] *See* Nawara, *supra* note 5, at 609–18.

constitutional "mechanism"[131] for catching potential errors that threaten the rights of criminal defendants.

[131] Williams v. Illinois, 567 U.S. 50, 118–19 (2012) (Kagan, J., dissenting).