ARTIFICIAL INTELLIGENCE IN THE COURTROOM: FORENSIC MACHINES, EXPERT WITNESSES, AND THE CONFRONTATION CLAUSE

Ian Maddox[1]

ABSTRACT

From traditional methods like ballistics and fingerprinting, to the probabilistic genotyping models of the twenty-first century, the forensic laboratory has evolved into a cutting-edge area of scientific exploration. This rapid growth in forensic technologies will not stop here. Considering recent developments in artificial intelligence ("AI"), future forensic tools will likely become increasingly sophisticated. To be sure, AI-enabled forensic tools are far from theoretical; AI applications in the forensic sciences have already emerged in practice. Machine learning-enabled acoustic gunshot detectors, facial recognition software, and a variety of pattern recognition learning models are already disrupting law enforcement operations across the country. Soon, criminal defendants will need to learn how to navigate a courtroom dominated by AI-enabled expert systems. Unfortunately, there is little guidance in the caselaw or in the Federal Rules of Evidence on how exactly criminal defendants should approach AI as evidence in the courtroom. Although a handful of scholars have taken up the task of exploring the intersection of AI and evidence law, these studies have primarily focused on issues in authentication or issues with applying the *Daubert* standard to AI evidence.

This study contributes to this ongoing exploration of AI in the courtroom by providing an analysis of the rights of criminal defendants facing AI-generated testimony under the Confrontation Clause of the Sixth Amendment. This study will illustrate that, in a future where AI-enabled forensic tools are increasingly used to inculpate defendants in criminal prosecutions, the right to confrontation will become increasingly eroded. This is largely because courts have carved out a broad "machine-generated data" exception to the Confrontation Clause. Under this exception, data generated by a sufficiently autonomous machine will fall outside the ambit of constitutional protection. The rationale is that such

[1] Ian Maddox, J.D., 2023, University of North Carolina School of Law; B.A., 2018, Johns Hopkins University. Many thanks to Professor Andrew Chin for helpful feedback and comments. The author is currently an Associate at Skadden, Arps, Slate, Meagher & Flom (the "Firm"). The author's views and the statements made therein do not necessarily reflect the views of the Firm or any of its clients.

transmissions are too autonomous to be attributed to any human actor, and the Confrontation Clause protects only statements made by a human rather than a machine learning model. This exception to the right to confrontation is significant. Practically, these limitations could have a measurable negative impact on a defendant's capacity to test the reliability of an AI model in court. Normatively, this study illustrates that, in a world where AI algorithms proffer inculpatory evidence of criminal wrongdoing, the right to confrontation adds little value for criminal defendants. As courts and scholars reinterpret and refine the rules of evidence to better reflect technological realities, some attention should be given to the proper place of the right to confrontation.

ARTIFICIAL INTELLIGENCE IN THE COURTROOM: FORENSIC MACHINES, EXPERT WITNESSES, AND THE CONFRONTATION CLAUSE

TABLE OF CONTENTS

INTRODUCTION

Forensic science has rapidly changed over the past several decades.[2] In the early twentieth century, traditional methods analyzing ballistics, bite marks, hair and fiber, handwriting, and fingerprints rose to prominence.[3] Beginning in the mid-to-late twentieth century, a new generation of forensic tools emerged.[4] These tools include gas chromatographs, breath readers, DNA typing, location tracking, and data mining.[5] Many of these forensic machines have been lauded for their accuracy and apparent objectiveness, with some commentators even labeling them "truth machines."[6]

This rapid growth in forensic technologies will not stop here. With recent developments in artificial intelligence ("AI"), future forensic tools will likely become increasingly sophisticated. To be sure, AI-enabled forensic tools are far from theoretical; they have

---

[2] *See* Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CAL. L. REV. 721, 722–44 (2007) (tracing developments in modern forensics); Andrea Roth, *Trial by Machine*, 104 GEO. L.J. 1245, 1253–69 (2016) [hereinafter, Roth, *Trial by Machine*] (cataloguing the growing use of forensic machines in criminal trials).

[3] Murphy, *supra* note 2, at 726; Jim Norton et al., *Flawed Forensics: Statistical Failings of Microscopic Hair Analysis*, 13 SIGNIFICANCE 26, 26–29 (2016); Jennifer L. Mnookin, *Scripting Expertise: The History of Handwriting Identification Evidence and the Judicial Construction of Reliability*, 87 VA. L. REV. 1723, 1797 (2001); NATIONAL INSTITUTE OF JUSTICE, THE FINGERPRINT SOURCEBOOK 1–16 (U.S. Dep't of Just. 2011); N. Balachander et al., *Evolution of Forensic Odontology: An Overview*, 7 J. PHARM. BIOALLIED SCI. 176, 176–80 (2015); John F. Fox, Jr., *The Birth of the FBI's Technical Laboratory*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/history/history-publications-reports/the-birth-of-the-fbis-technical-laboratory1924-to-1935 [https://perma.cc/C4UT-5UE7] (last visited Apr. 9, 2024).

[4] *See* Murphy, *supra* note 2, at 723; *infra* note 5 and accompanying text.

[5] Murphy, *supra* note 2, at 728; Roth, *Trial by Machine*, supra note 2, at 1259–60; Harold McNair, *A History of Gas Chromatography*, 28 LCGC N. AM. 138, 138 (2010); Linda Castro & Samuel Fosso Wamba, *An Inside Look at RFID Technology*, 2 J. TECH. MANAG. INNOVATION 128, 128 (2007); *Global Positioning System History*, NASA (Aug. 7, 2012), https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS_History.html [https://perma.cc/RRR4-3WB3].

[6] *See* Roth, *Trial by Machine*, *supra* note 2, at 1247, 1252 ("American courts and law enforcement pride themselves on embracing a number of crime-detecting gadgets touted as 'truth machines'—from daguerreotype imaging to the Drunk-O-Meter to DNA."); John Ashcroft, Attorney General, *News Conference on DNA Initiative at DOJ Conference Center*, U.S. DEP'T OF JUST. (Mar. 4, 2002), https://www.justice.gov/archive/ag/speeches/2002 [https://perma.cc/EAQ7-U57Y] ("DNA technology has proven itself to be the truth machine of law enforcement, ensuring justice by identifying the guilty and exonerating the innocent.").

already emerged in practice. Law enforcement is already using face recognition tools like Clearview AI,[7] Oosto's Vision AI[8] and Neurala Deep Learning,[9] as well as AI-enabled DNA typing software,[10] acoustic gunshot detectors like ShotSpotter,[11] and voice recognition software like SpeechPro.[12] Still, other forensic tools have yet to hit the market, including "smart-breathalyzers,"[13] along with machine learning models used for bullet

[7] James Clayton & Ben Derico, *Clearview AI Used Nearly 1m Times by US Police*, BBC (Mar. 27, 2023), https://www.bbc.com/news/technology-65057011 [https://perma.cc/S333-6S9J]; Amanda Levendowski, *Resisting Face Surveillance with Copyright Law,* 100 N.C. L. REV. 1015, 1017 (2022) (noting that, "[i]n less than three years, Clearview AI systemically copied three billion photographs to create face recognition tools for six hundred police departments").

[8] *Real-Time Facial Recognition Using Your Existing Cameras*, OOSTO (last visited Apr. 1, 2024), https://oosto.com/ [https://perma.cc/ELC8-SG5H] [hereinafter *Oosto's Real-Time Facial Recognition*]; *Law Enforcement*, OOSTO, https://oosto.com/wp-content/uploads/2023/03/oosto-law-enforcement-datasheet.pdf (last visited Apr. 15, 2023) [hereinafter *Oosto and Law Enforcement*].

[9] *Improve Quality Inspections with Vision AI Software*, NEURALA, https://www.neurala.com/ [https://perma.cc/J9LV-PCAD]; Haley Britzky, *Facial Recognition Tech Could Be Coming to Police Body Cams*, AXIOS (July 17, 2017), https://www.axios.com/2017/12/15/facial-recognition-tech-could-be-coming-to-police-body-cams-1513304241 [https://perma.cc/3HT4-N3A9].

[10] *See, e.g.,* Dan Bernardi, *Forensic Scientists Design the First Machine Learning Approach to Forensic DNA Analysis*, SYRACUSE UNIV. STEM NEWS (July 28, 2021), https://news.syr.edu/blog/2021/07/28/forensic-scientists-design-the-first-machine-learning-approach-to-forensic-dna-analysis/ [https://perma.cc/QT2Q-DJQF]; Michael A. Marciano & Jonathan D. Adelman, *Developmental Validation of PACE™*, 43 FORENSIC SCI. INT'L 1, 1–2 (2019).

[11] *ShotSpotter, Save Lives and Find Critical Evidence with the Leading Gunshot Detection System,* SOUNDTHINKING (last visited Apr. 1, 2024), https://www.soundthinking.com/law-enforcement/gunshot-detection-technology/ [https://perma.cc/2P79-V4E4]; *ShotSpotter's Latest U.S. Patent Enables Major Advancement in Machine Learning Accuracy for Its Gunshot Detection Technology*, SOUNDTHINKING, https://www.soundthinking.com/press-releases/shotspotters-latest-u-s-patent-enables-major-advancement-in-machine-learning-accuracy-for-its-gunshot-detection-technology/ [https://perma.cc/F88D-4SLK] (last visited Apr. 1, 2024) [hereinafter, *ShotSpotter's Latest U.S. Patent*].

[12] Ryan Gallagher, *Watch Your Tongue: Law Enforcement Speech Recognition System Stores Millions of Voices*, SLATE (Sept. 20, 2012, 1:58 PM), https://slate.com/technology/2012/09/speechpro-voicegrid-nation-voice-recognition-software-for-use-by-law-enforcement.html [https://perma.cc/E2N7-6C4N]*; SpeechPro Participates in NIST Speaker Recognition i-Vector Machine Learning Challenge*, PRWEB (June 17, 2014), https://www.prweb.com/releases/2014/07/prweb12024102.htm [https://perma.cc/6TYS-HBPB] [hereinafter *SpeechPro*]; Dina Temple-Raston, *Voice 'Fingerprints' Change Crime-Solving*, NPR (Jan. 28, 2008), https://www.npr.org/templates/story/story.php?storyId=18479095 [https://perma.cc/L3FM-GHLX].

[13] Kirstin Aschbacher et al., *Machine Learning Prediction of Blood Alcohol Concentration: A Digital Signature of Smart-Breathalyzer Behavior*, 4 NJP DIGITAL MED. 1, 1 (2021).

matching, shoeprint identification, fingerprinting, and other pattern recognition applications.[14]

Soon, criminal defendants will need to learn how to navigate a courtroom dominated by AI-enabled expert systems. Unfortunately, there is little guidance in the caselaw or in the Federal Rules of Evidence on how litigants should approach AI as evidence in the courtroom.[15] Nevertheless, several scholars have taken up the task, including Professors Paul W. Grimm, Maura R. Grossman, and Gordon V. Cormack. In a comprehensive primer on artificial intelligence as evidence, these scholars tackled novel questions of authentication, relevance, and other discrete issues in admissibility.[16] Other scholarship on AI as evidence has focused narrowly on issues relating to expert testimony under the *Daubert* standard.[17] Still other scholarly works have centered their analyses on exploring the many authentication issues implicated by the use of AI in the courtroom.[18]

---

[14] *See, e.g.*, Alicia Carriquiry et al.*, Machine Learning in Forensic Applications,* 16 SIGNIFICANCE 29, 29–35 (2019); Eric Hare, Heike Hofmann & Alicia Carriquiry, *Algorithmic Approaches to Match Degraded Land Impressions*, 16 LAW PROBABILITY & RISK 203, 203–04 (2017); Bailey Kong et al., *Cross-Domain Image Matching with Deep Feature Maps*, 127 INT'L J. COMPUT. VISION 1738, 1738–40 (2019); Oscar García-Olalla et al., *Textile Retrieval Based on Image Content from CDC and Webcam Cameras in Indoor Environments*, 18 SENSORS 1, 1–4 (2018).

[15] *Cf.* Hon. Paul W. Grimm et al., *Artificial Intelligence as Evidence*, 19 NW. J. TECH. & INTELL. PROP. 9, 84 (2021) ("To date, there have been few, if any, court decisions squarely addressing th[e] topic [of admissibility of AI evidence] . . . and the cases that have referenced AI evidence often have done so in a cursory or tangential manner."); FED R. EVID. 901 advisory committee's note to 2011 amendment (failing to distinguish between AI and other process- or system-based evidence); FED R. EVID. 702 advisory committee's note to 2000 amendment (failing to distinguish between AI and other scientific evidence).

[16] *See generally* Grimm et al., *supra* note 15 (exploring issues in admissibility for AI, including biased data, robustness of testing, monitoring for function creep, and transparency and explainability). *See also* Hon. Paul W. Grimm, *New Evidence Rules and Artificial Intelligence,* 45 LITIGATOR'S TOOLBOX 6, 6 (2018).

[17] *See, e.g.*, Patrick W. Nutter, *Machine Learning Evidence: Admissibility and Weight*, 21 U. PA. J. CONST. L. 919, 922 (2019). *See also* Pamela S. Katz*, Expert Robot: Using Artificial Intelligence to Assist Judges in Admitting Scientific Expert Testimony*, 24 ALB. L.J. SCI. & TECH. 1, 1 (2014).

[18] *See, e.g*, Agnieszka McPeak, *The Threat of Deepfakes in Litigation: Raising the Authentication Bar to Combat Falsehood*, 23 VAND. J. ENT. & TECH. L. 433, 434 (2021); Rebecca A. Delfino, *Deepfakes on Trial: A Call to Expand the Trial Judge's Gatekeeping Role to Protect Legal Proceedings from Technological Fakery*, 74 HASTINGS L.J. 293, 332 (2023) (noting that "none of the Federal Rules of Evidence or their companion common-law theories are sufficient to address the significant challenges that deepfakes present").

This study contributes to this ongoing discussion on AI in the courtroom by analyzing the rights of criminal defendants facing AI-generated testimony under the Confrontation Clause of the Sixth Amendment.[19] The Confrontation Clause provides criminal defendants with the right "to be confronted with the witnesses against him."[20] Where a witness merely acts as a "surrogate" witness, parroting the out-of-court statements of *ex parte* accusers, the idea is that a criminal defendant should be able to call his or her *ex parte* accuser to the witness stand for cross-examination.[21] A violation will occur where a statement is "testimonial"—that is, a violation will occur where the circumstances objectively indicate that the "primary purpose" of the statement is to aid in a criminal prosecution, to accuse a targeted individual, or to be used as testimony at trial.[22] Further, the given statement must be an out-of-court statement offered to prove the truth of the matter asserted; meaning, the statement must be hearsay.[23]

This case study will illustrate that in a future where AI-enabled forensic tools are increasingly used in criminal prosecutions, the right to confrontation will become increasingly eroded. This is for two reasons. First, the test courts employ to determine whether a statement is "testimonial" is greatly limited in its ability to provide protection in cases involving expert testimony and forensic testing.[24] Second, courts have carved out a broad "machine-generated data" exception to the hearsay rule as it is articulated under the Confrontation Clause.[25] Under this exception, data generated by a sufficiently autonomous machine will fall outside the ambit of constitutional protection.[26] Both these

[19] This Paper also contributes to the ongoing study of the Confrontation Clause as it intersects with forensic science. *See, e.g.*, Jennifer Mnookin & David Kaye, *Confronting Science: Expert Evidence and the Confrontation Clause*, 2012 SUP. CT. REV. 99 (2012); Jennifer L. Mnookin, *Expert Evidence and the Confrontation Clause After Crawford v. Washington*, 15 J.L. & POL'Y 791 (2007); Brian Sites, *Machines Ascendant: Robots and the Rules of Evidence*, 3 GEO. L. TECH. REV. 1, 6 (2018); Nicholas Klaiber, Note, *Confronting Reality: Surrogate Forensic Science Witnesses Under the Confrontation Clause*, 97 VA. L. REV. 199 (2011).

[20] *See* U.S. CONST. amend. VI.

[21] *See* Crawford v. Washington, 541 U.S. 36, 50 (2004); Bullcoming v. New Mexico, 564 U.S. 647, 652 (2011).

[22] *See* Davis v. Washington, 547 U.S. 813, 822 (2006); Michigan v. Bryant, 562 U.S. 344, 358 (2011); Williams v. Illinois, 567 U.S. 50, 82 (2012).

[23] *Crawford*, 541 U.S. at 53, 59 n.9.

[24] *See infra* Section II.A.

[25] *See infra* Section II.B.

[26] *See id.*

limits work in tandem to frustrate the Confrontation Clause in a future where AI-enabled forensic tools dominate criminal prosecutions.

This outcome is significant. As a practical matter, these limitations could have a measurable negative impact on a defendant's capacity to test the reliability of an AI model in court.[27] The right to confrontation's limited scope reduces a defendant's ability to test the reliability of evidence generated by AI. Normatively, the implications of this study are more far-reaching. In a world where AI algorithms proffer inculpatory evidence of criminal wrongdoing, the right to confrontation adds little value for criminal defendants.[28] This is notable considering that "the [Confrontation] Clause's ultimate goal is to ensure reliability of evidence."[29] As courts and scholars reinterpret and refine the rules of evidence to better reflect technological realities, some attention should be given to the proper place of the right to confrontation.

To ensure that defendants are provided with adequate constitutional protections and sufficient means to test the reliability of AI evidence, this Paper advances several different proposals. First, in the short term, courts should ensure that existing *ex ante* gatekeeping standards, such as the rules governing authentication of computational evidence and expert testimony, are applied with sufficient rigor.[30] In the longer term, jurists might consider revising, reinterpreting, or amending the federal rules to supply criminal

[27] While it is true that there are other means of testing reliability other than cross-examination, there is evidence that an erosion of confrontation rights will negatively impact a defendant's ability to challenge the prosecution's case. *See infra* Section III.A. At bottom, the right to cross-examination of a human witness involved in the production of the AI-generated data can provide litigants with unique opportunities to test forensic analysts for truthfulness, bias, and inconsistencies in front of a sitting jury. *See id.* Further, *ex ante* gatekeeping mechanisms such as authentication and the rules governing expert testimony are frequently criticized as being limited, overly discretionary, and inconsistently applied. *See Id.*; Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 2014, 2030–35 (2017) [hereinafter, Roth, *Machine Testimony*]; Grimm et al., *supra* note 15, at 94; Jeffrey Bellin & Andrew Guthrie Ferguson, *Trial by Google: Judicial Notice in the Information Age*, 108 NW. U. L. REV. 1137, 1137–43, 1161 (2014); Jim Hilbert, *The Disappointing History of Science in the Courtroom: Frye, Daubert, and the Ongoing Crisis of "Junk Science" in Criminal Trials*, 71 OKLA. L. REV. 759, 763 (2019); Edward K. Cheng & G. Alexander Nunn, *Beyond the Witness: Bringing a Process Perspective to Modern Evidence Law*, 97 TEX. L. REV. 1077 (2019).

[28] *See infra* Part II.

[29] *Crawford*, 541 U.S. at 61.

[30] *See infra* Section III.C.

defendants with a right to validation testing for AI evidence.[31] In many ways, validation testing is the "computational" analog to human reliability testing via cross-examination.[32]

This Paper proceeds in three parts. Part I will provide a brief background on AI-enabled forensic tools and the legal framework used by courts in assessing Confrontation Clause claims. Part II will demonstrate the limited ability of the Confrontation Clause to provide protection to criminal defendants in cases involving AI. This Part will also include several illustrative hypotheticals. Finally, Part III will present the implications of this study and propose several recommendations for reform to scholars, practitioners, and jurists.

I. A BACKGROUND ON FORENSIC MACHINES, AI, AND THE RIGHT TO CONFRONTATION

Before proceeding to the analysis, a brief introduction into AI and the right to confrontation is necessary. This Part will provide background on AI-enabled forensic tools and the legal framework for analyzing Confrontation Clause challenges. First, this Part will describe the emergence of AI applications in the forensic sciences. Next, this Part will detail the legal framework courts employ to assess the validity of a Confrontation Clause challenge.

A. Applications of Artificial Intelligence in Forensic Science

AI is a branch of computer science that encompasses "a number of research topics and underlying technologies aimed at furthering the application of computers to intellectual tasks, as well as the tasks themselves."[33] Included under this umbrella term are logical rules and knowledge representation, as well as applications in machine learning.[34] Logical rules and knowledge representation are AI systems that involve "providing a computer with a series of rules that represent the underlying logic and knowledge of whatever

[31] *See id.*

[32] *See id.*

[33] Grimm et al., *supra* note 14, at 15. This Paper focuses on artificial "narrow" intelligence, which are AI models that "use purpose-built hardware and/or software systems that seek to emulate (or better) human performance at a single, well-defined task." *Id.* at 16. Artificial "general" intelligence has yet to become a reality; this form of AI "refers to a computer's ability to rival or exceed human performance at a full complement of cognitive tasks." *Id.*

[34] Harry Surden, *Artificial Intelligence and Law: An Overview*, 35 GA. ST. U. L. REV. 1305, 1311, 1316 (2019) [hereinafter Surden, *Artificial Intelligence and Law*].

activity the programmers are trying to model and automate." In contrast, machine learning involves "detecting useful patterns in large amounts of data."[35]

Many of the applications of AI in the forensic context use machine learning algorithms.[36] Machine learning is concerned with the development of computer programs that are capable of "learn[ing] from experience," which allows for improvements in performance with the passage of time.[37] These AI systems use learning algorithms to recognize patterns in data sets in order to automate complicated tasks or to make predictions.[38] Machine learning algorithms have demonstrated a capacity to learn and master tasks previously thought to be too complex for machines, and many of these models are able to "see" patterns beyond the limits of human perception.[39] Future applications of this technology in forensics will allow for a far-greater ability to accurately and objectively detect forensic source matches.[40]

Many forensic scientists are already exploring potential applications of AI in the forensic context.[41] These breakthroughs hold great promise for enhancing the accuracy of a variety

---

[35] *Id.* at 1311.

[36] *See, e.g., Neurala Announces Breakthrough Update to Award-Winning Deep Neural Network Technology*, NEURALA (May 9, 2018), https://www.neurala.com/press-releases/neurala-announces-breakthrough-update-to-award-winning-deep-neural-network-technology (using deep learning) [https://perma.cc/TZY5-PX4W]; Jinny X. Zhang et al., *A Deep Learning Model for Predicting Next-Generation Sequencing Depth from DNA Sequence*, 12 NATURE COMMC'N 1, 1 (2021) (using deep learning); Carriquiry et al., *supra* note 14, at 33–35 (using random forests). *But cf.* Surden, *Artificial Intelligence and Law*, *supra* note 34, at 1316–17 (describing the possibility of a rules-based/knowledge representation system that "might allow later users to make automated, expert-level diagnoses using the encoded knowledge").

[37] Harry Surden, *Machine Learning and Law*, 89 WASH. L. REV. 87, 89 (2014) [hereinafter Surden, *Machine Learning and Law*].

[38] *Id.*

[39] Bradley J. Erickson et al., *Machine Learning for Medical Imaging*, 37 RADIOGRAPHICS 505, 505–13 (2017).

[40] *See infra* notes 40–57 and accompanying text.

[41] *See, e.g.*, Bernardi, *supra* note 9; Marciano & Adelman, *supra* note 9, at 1–2; Nur-A-Alam et al., *An Intelligent System for Automatic Fingerprint Identification Using Feature Fusion by Gabor Filter and Deep Learning*, 95 COMPUT. & ELEC. ENG'R 1, 1–3 (2021); Aschbacher et al., *supra* note 12, at 1. *Cf.* Andrew Carroll & Pi-Chuan Chang, *Improving the Accuracy of Genomic Analysis with DeepVariant 1.0*, GOOGLE RESEARCH (Sept. 18, 2020), https://ai.googleblog.com/2020/09/improving-accuracy-of-genomic-analysis.html [https://perma.cc/YR7Y-HUBJ].

of forensic subdisciplines, including DNA typing, ballistics, fiber analysis, and speech recognition.[42] For instance, Professors Michael Marciano and Jonathan Adelman at Syracuse University's Forensic and National Security Sciences Institute recently developed a machine learning approach to DNA typing that promises reduced error rates in DNA mixtures originating from multiple contributors.[43] These professors trained their algorithm on thousands of mixture samples; gradually, the algorithm learned to distinguish samples containing DNA from varying sets of people.[44]

Future developments are not limited to DNA evidence. In April 2019, a research team at Iowa State University unveiled a machine learning algorithm capable of recognizing complex patterns of physical evidence.[45] This algorithm improved the statistical reliability of bullet matching—the age-old ballistics process of comparing bullets obtained from a crime scene.[46] Similarly, in January 2019, researchers at UC Irvine and Carnegie Mellon used AI to better conduct shoeprint analysis.[47] With this pattern recognition tool, these researchers were able to readily determine the model and mark of shoe impressions left at the crime scene.[48] This same approach was mirrored by researchers at the University of León in Spain, who developed a pattern-recognition tool that used machine learning to identify textile materials in police photographs.[49]

To be sure, applying AI in the forensic context is far from theoretical. In practice, its adoption has already begun, particularly in the forensic subdisciplines of face and speech recognition.[50] Police departments across the country use AI-enabled voice recognition software from SpeechPro, a company that uses machine learning to identify voice prints.[51]

---

[42] *See infra* notes 42–57 and accompanying text.

[43] Bernardi, *supra* note 9; Marciano & Adelman, *supra* note 9, at 1–2; Maria-Alexandra Katsara et al., *Evaluation of Supervised Machine-Learning Methods for Predicting Appearance Traits from DNA*, 53 FORENSIC SCI. INT'L 1, 1–2 (2021).

[44] Chris Baraniuk, *The New Weapon in the Fight Against Crime*, BBC (Mar. 3, 2019), https://www.bbc.com/future/article/20190228-how-ai-is-helping-to-fight-crime [https://perma.cc/228D-233S]; *see also* Bernardi, *supra* note 9.

[45] Carriquiry et al., *supra* note 13, at 29–35.

[46] *Id.*; Hare et al, *supra* note 13, at 203–04.

[47] Kong et al., *supra* note 13, at 1738–40.

[48] *Id.*

[49] Baraniuk, *supra* note 43. Using the texture of the textile object—a blanket on a bed, for instance—the image retrieval system will identify the common source. *See* García-Olalla et al., *supra* note 13, at 1–4.

[50] *See infra* notes 50–57 and accompanying text.

[51] Gallagher, *supra* note 12; *SpeechPro*, *supra* note 12; Temple-Raston, *supra* note 12.

Further, advances in machine learning, acoustic sensing, and GPS technology have led to the development of ShotSpotter, a product that provides police officers with the means to more accurately detect and locate gunshot incidents.[52] Further, many private companies sell AI-enabled face recognition technologies to law enforcement.[53] Examples include Clearview AI,[54] Oosto's Vision AI,[55] Neurala Deep Learning,[56] Microsoft's Face API,[57] and Amazon's Rekognition.[58]

Notably, outside of the forensics context, machine learning is already widely used in the criminal justice system; its further expansion into forensics would be a natural extension of this trend. For pretrial release and sentencing decisions, many judges rely on risk-assessment instruments that use machine learning to predict propensity and the likelihood of recidivism.[59] Similarly, many law enforcement agencies use AI for predictive policing. For example, to better identify crime hotspots, many departments rely on products like

[52] Temple-Raston, *supra* note 12; *ShotSpotter FAQ August 2018*, SHOTSPOTTER (Aug. 2018), https://www.shotspotter.com/wp-content/uploads/2018/08/FAQ_Aug_2018.pdf; *ShotSpotter's Latest U.S. Patent*, *supra* note 11.

[53] *Cf.* Levendowski, *supra* note 7, at 1020 ("Nearly a decade of scholarship rooted in lived experiences reveals an urgent need for a federal law banning the use of face surveillance by law enforcement.").

[54] Clayton & Derico, *supra* note 7.

[55] *Oosto's Real-Time Facial Recognition*, *supra* note 8; *Oosto and Law Enforcement*, *supra* note 8.

[56] *Engadget*, *supra* note 9; Britzky, *supra* note 9.

[57] *FaceAPI*, AZURE, https://azure.microsoft.com/en-au/products/cognitive-services/face/ [https://perma.cc/WB7Y-B3UY] (last visited Apr. 8, 2024). This technology is no longer sold to law enforcement. *See* Ari Levy, *Microsoft Says It Won't Sell Facial Recognition Software to Police Until There's a National Law 'Grounded in Human Rights'*, CNBC (Jun. 11, 2020, 1:37 PM), https://www.cnbc.com/2020/06/11/microsoft-says-will-not-sell-facial-recognition-software-to-police.html [https://perma.cc/L8AV-TF57].

[58] *Amazon Rekognition*, AMAZON WEB SERVS., https://aws.amazon.com/rekognition/ [https://perma.cc/C8TW-QJU4] (last visited Apr. 8, 2024). Like Microsoft, Amazon has stopped selling this technology to law enforcement. *See* Karen Weise, *Amazon Indefinitely Extends a Moratorium on the Police Use of Its Facial Recognition Software*, N.Y. TIMES (Aug. 1, 2021), https://www.nytimes.com/2021/05/18/business/amazon-police-facial-recognition.html [https://perma.cc/DHP9-D3VN].

[59] Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 WASH. U.L. REV. 1109, 1120–21 (2017) ("Today, actuarial prediction impacts almost all aspects of the criminal justice system, from the initial bail decision to the final parole release."). This includes the Correctional Offender Management Profiling for Alternative Sanctions ("COMPAS") algorithm. *See* Doaa Abu Elyounes, *Bail or Jail? Judicial Versus Algorithmic Decision-Making in the Pretrial System*, 21 COLUM. SCI. & TECH. L. REV. 376, 418 (2020).

PredPol Policing Technology[60] and Alvea's Hunchlab,[61] which use machine learning algorithms. Still, other AI models in predictive policing such as Palantir allow law enforcement to put together target lists of possible perpetrators or victims of gun violence through an analysis of individual historical data.[62] Widespread application of AI in the forensic sciences is still forthcoming, but these trends suggest that its rise to prominence is only a matter of time.

Although AI-enabled forensic tools hold great promise for improved accuracy in forensic testing, such developments are not without risks.[63] The reliability of a machine learning model is heavily dependent on the quality of the data it is trained on.[64] Biased or

[60] *See* Mirko Bagaric et. al., *The Solution to the Pervasive Bias and Discrimination in the Criminal Justice System: Transparent and Fair Artificial Intelligence*, 59 AM. CRIM. L. REV. 95, 109–10 (2022) ("Several jurisdictions, including Birmingham, also adopted PredPol, a system that was first used in Los Angeles, California.").

[61] Ashley S. Deeks, *Predicting Enemies*, 104 VA. L. REV. 1529, 1542–45 (2018).

[62] *Id.*; Ali Winston, *Palantir Has Secretly Been Using New Orleans to Test Its Predictive Policing Technology*, VERGE (Feb. 27, 2018, 3:25 PM), https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd [https://perma.cc/W9FJ-S5Y3]; *Artificial Intelligence & Machine Learning*, PALANTIR, https://www.palantir.com/offerings/ai-ml/ [https://perma.cc/B3TR-A5Q9] (last visited Apr. 8, 2024). Many police departments have purchased Avista Smart Sensor, a product that uses machine learning to scan surveillance footage for signs of potential criminals and reports those findings to law enforcement. *See* Russell Nichols, *Smart Cameras Aim to Stop Crimes Before They Occur*, GOV'T TECH. (Oct. 26, 2010), https://www.govtech.com/public-safety/smart-cameras-aim-to-stop-crimes-before-they-occur.html [https://perma.cc/A7FB-Q3S3]; Roth, *Trial by Machine*, *supra* note 2, at 1258.

[63] *See, e.g.*, Levendowski, *supra* note 7, at 1015 (describing misidentification by a face recognition algorithm).

[64] *See What is Machine Learning?*, IBM, https://www.ibm.com/topics/machine-learning [https://perma.cc/3MTF-WNRB] (last visited Apr. 8, 2024); Adrienne Grzenda et al., *Evaluating the Machine Learning Literature: A Primer and User's Guide for Psychiatrists*, 178 AM J. PSYCHIATRY 715, 722–23 (2021) ("Model accuracy and validity are highly dependent on the availability of large amounts of high-quality training data, which can be expensive and time-consuming to generate."); Grimm et al., *supra* note 15, at 42. Organizing and integrating this collected data can create further opportunities for error: "[s]ignificant care must be taken to determine the quantitative and qualitative equivalence of shared features across time, location, and instrumentation when integrating data sets from different sites or collection protocols." *See* Grzenda et al., *supra*, at 723. Particular attention must also be given to the labeling of the training data containing the input and output variables in supervised learning models. *See Id.* at 716 ("[A] supervised algorithm can only be as accurate as the labels provided for training.").

inaccurate data will yield an unreliable result.[65] As a general matter, larger datasets of training data are preferable, as "[s]mall training data sets may yield highly inaccurate predictions when applied to new data."[66] A disparity in geographic or demographic coverage may "negatively influence the generalizability of the training data to the general population."[67] Recent experience with machine learning applications in facial recognition software and health care have revealed that these algorithms are prone to racial bias.[68]

It is also worth noting that even an AI model will not necessarily obviate the risk of negligence or malfeasance in collecting or maintaining a test sample. AI models that aid forensic scientists with techniques like bullet matching, hair comparison, shoeprint analysis, and DNA typing rely on human investigators to properly collect and maintain the physical evidence found at the source site.[69] This necessarily introduces human error into the analysis.[70] To illustrate, issues in DNA collection and maintenance can occur from "using the same instrument to gather more than one sample;" "having the examiner herself contaminate the sample with her own DNA through saliva, sweat, or dandruff;" or

[65] Jenni A. M. Sidey-Gibbons & Chris J. Sidey-Gibbons, *Machine Learning in Medicine: A Practical Introduction*, 19 BMC MED. RSCH. METHODOLOGY 1, 17 (2019); Grzenda et al., *supra* note 64, at 723.

[66] Grzenda et al., *supra* note 64, at 722–23.

[67] *Id.*

[68] *Id.*; *What is Machine Learning?*, *supra* note 64 ("Instances of bias and discrimination across a number of machine learning systems have raised many ethical questions regarding the use of artificial intelligence."); *see also* Levendowski, *supra* note 7, 1016–26; Margaret Hu, *Algorithmic Jim Crow*, 86 FORDHAM L. REV. 633, 634–46 (2017); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671, 671–77 (2016); Laura M. Moy, *A Taxonomy of Police Technology's Racial Inequity Problems*, 2021 U. ILL. L. REV. 139, 141 (2021). It is also notable that the datasets underlying DNA typing have been criticized for their disparate racial composition. *See* Erin Murphy & Jun H. Tong, *The Racial Composition of Forensic DNA Databases*, 108 CAL. L. REV. 1847, 1851–52 (2020); PATRICK K. LIN, MACHINE SEE, MACHINE DO: HOW TECHNOLOGY MIRRORS BIAS IN OUR CRIMINAL JUSTICE SYSTEM 126 (2021) (noting that "racial disparities in arrests and imprisonment ultimately translates into the disproportionate collection of Black and Latinx DNA."). A 2020 study of CODIS, conducted across seven different states, found that "although White people make up 62% of the total U.S. population, they make up only 49% of the disclosed DNA database." Murphy & Tong, *supra*, at 1851–52. In contrast, "although Black people make up only 13% of the U.S. population, they contribute 34% of samples to the disclosed DNA database." *Id.* at 1851.

[69] This analysis would differ should autonomous machines wholly take the place of crime scene investigators.

[70] *See* Andrea Roth, *Defying DNA: Rethinking the Role of the Jury in an Age of Scientific Proof of Innocence*, 93 B.U. L. REV. 1643, 1676–78 (2013).

even through "purposeful contamination."[71] These test sample errors will inevitably affect the resulting accuracy of the AI model's readout.[72]

Other AI pitfalls include its lack of methodological transparency, which can serve as a barrier to thorough scrutiny. Many AI models are criticized for being "opaque" and "black boxes."[73] In machine learning, "[t]he meaning of model parameters and feature relationships can be difficult to determine, and in cases where a model errs, it is difficult to determine why."[74] To be sure, not all AI systems are so inscrutable: "[s]ome automated learned models are more transparent than others, for example, if the feature engineering is straightforward and the method of combining evidence from the features is not too complicated."[75] Nevertheless, there are certainly AI models that are "black boxes," including some state-of-the-art image recognition and voice recognition models.[76] This can create a barrier for criminal defendants wishing to thoroughly scrutinize a model's methodology.[77]

B. Background on the Confrontation Clause

The Confrontation Clause provides a criminal defendant with "the right . . . to be confronted with the witnesses against him."[78] This right is commonly implicated where a criminal defendant is accused of a crime via an out-of-court statement "read in court in lieu of live testimony," and where that defendant demands that the author of the

[71] *Id.*

[72] *See* Young v. United States, 63 A.3d 1033, 1046 n.49 (D.C. 2013) ("It is axiomatic . . . that if a human being does not enter correct information, the output from a computer means nothing. This principle is known in computer science as 'garbage in, garbage out' and is traced back to Charles Babbage . . . .").

[73] Grzenda et al., *supra* note 63, at 725; Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085, 1089–90 (2018) (noting that some scholars refer to algorithms as "secret," "opaque," and "black boxes").

[74] Grzenda et al., *supra* note 73, at 725.

[75] Grimm et al., *supra* note 14, at 29.

[76] *Id.* at 30.

[77] On the other hand, interpretability and explainability may not be necessary for ensuring reliability. Validation testing can provide useful insights into reliability without delving into the internal processes of the AI model. *See* Grzenda et al., *supra* note 64, at 726. For more discussion on validation testing, see *infra* Section III.C.

[78] *See* U.S. CONST. amend. VI.

statement be "brought before him face to face."[79] In such situations, the clause grants a defendant the right to "confront" his or her *ex parte* accusers by cross-examination.[80]

To not grant a defendant this right would allow an accuser to launch shielded attacks against the defendant from afar. To illustrate, in *Crawford v. Washington*,[81] the Supreme Court held that the Confrontation Clause was violated where an *ex parte* witness's accusatory statements made to police were introduced at trial.[82] There, a defendant was tried with assault and attempted murder.[83] The *ex parte* witness—the defendant's wife—had offered statements to police that undermined the defendant's self-defense claim.[84] At trial, the prosecution sought to admit these statements under a hearsay exception.[85] The Court concluded that this testimony violated the Confrontation Clause.[86] The defendant could not "confront" his accuser via cross examination; marital privilege had prevented the defendant's wife from testifying.[87] Further, the Court noted that statements made to police fell within the core class of statements barred by the Confrontation Clause.[88]

The legal test courts employ to determine whether a criminal defendant's confrontation rights are violated is twofold. First, the inculpatory statement must be "testimonial" in nature.[89] Second, the inculpatory statement must be an out-of-court statement offered for the truth of the matter asserted.[90] The violation can be cured, however, if the prosecution shows that the declarant was unavailable and that the defendant had a prior opportunity to cross-examine the declarant.[91]

---

[79] Crawford v. Washington, 541 U.S. 35, 43 (2004) (quoting 1 J. STEPHEN, HISTORY OF THE CRIMINAL LAW OF ENGLAND 326 (1883)).

[80] *See id.* at 61.

[81] 541 U.S. 36 (2004).

[82] *Id.* at 68.

[83] *Id.* at 40.

[84] *Id.*

[85] *Id.* (noting that the prosecution attempted to introduce the evidence as "statements against penal interest").

[86] *Id.* at 68.

[87] *Id.* at 40 (noting that the defendant's wife "did not testify because of the state marital privilege").

[88] *Id.* at 52 (noting that "[s]tatements taken by police officers in the course of interrogations are also testimonial").

[89] *See id.* at 50–51.

[90] *See id.*

[91] *See generally id.*

First, a violation will only occur if the hearsay statement is "testimonial." Whether a statement is testimonial is not clearly delineated in the caselaw, and the test to determine a testimonial statement is commonly referred to as the "primary purpose" test.[92] As a general matter, a statement is "testimonial" if its primary purpose is to be used to inculpate a defendant at trial.[93] Discrete examples of testimonial statements under this test include "prior testimony at a preliminary hearing, before a grand jury, or at a former trial,"[94] statements to law enforcement in an interrogation,[95] and statements describing a criminal act.[96] Examples of non-testimonial statements include inconsistent statements used to impeach a declarant[97] and statements made to explain or clarify other admissible evidence.[98]

Second, for a statement to violate the Confrontation Clause, it must be an out-of-court statement offered for the truth of the matter asserted; that is, it must be hearsay.[99] Hearsay includes out-of-court statements that are written, spoken, or implied by conduct.[100] Accordingly, in the forensic machine context, "statements" include the entries in a database, procured reports of data, laboratory test results, and the opinions of other experts.[101] Whether the statement is offered for the truth of the matter asserted depends on the content of the statement and the reason for its introduction. Where the content of

---

[92] *See* Davis v. Washington, 547 U.S. 813, 822 (2006); *see infra* Section II.A and accompanying text.

[93] United States v. Saget, 377 F.3d 223, 228 (2d Cir. 2004), *supplemented*, 108 F. App'x 667 (2d Cir. 2004); *Crawford*, 541 U.S. at 51–52 (noting that "[v]arious formulations of this core class of 'testimonial' statements exist" and listing one formulation; namely, that statements are testimonial if they are "made under circumstances which would lead an objective witness reasonably to believe that the statement would be available for use at a later trial" (internal quotation marks and citation omitted)).

[94] *Crawford*, 541 U.S. at 68.

[95] *Id.* However, if the statement is made to help police with an emergency, then the statement is not testimonial. *See Davis*, 547 U.S. at 822.

[96] *See* United States v. Logan, 419 F.3d 172, 178 (2d Cir. 2005).

[97] Jackson v. Stovall, 467 F. App'x 440, 443–44 (6th Cir. 2012).

[98] *See Logan*, 419 F.3d at 178; United States v. Dipietro, No. S502CIR1237SWK, 2005 WL 1430483, at *1 n.1 (S.D.N.Y. June 17, 2005); United States v. Guzman, 754 F.2d 482, 487 (2d Cir. 1985).

[99] *See Crawford*, 541 U.S. at 50–51. Technically, this definition of hearsay is different than that under the Federal Rules of Evidence, since whether a statement is hearsay for confrontation purposes "depends upon 'the law of Evidence for the time being.'" *See id.* at 51 (quoting WIGMORE, EVIDENCE § 1397, at 101 (2d ed. 1923)). For the purposes of this paper, this distinction does not alter the analysis.

[100] *See* FED R. EVID. 801.

[101] *See id.*

the statement is a recitation of forensic test results, that statement is necessarily offered to prove the truth of the test results.[102]

In practice, Confrontation Clause concerns frequently arise in cases where the prosecution offers expert testimony. This is because, as a general matter, experts are allowed to rely on the statements of *ex parte* witnesses under the Federal Rules of Evidence. Pursuant to Rule 701, an expert need not have personal knowledge of a matter to testify about it at trial.[103] Further, under Rule 703, an expert may base his or her opinion on inadmissible facts and data, including inadmissible hearsay.[104] To be sure, under Rule 703, the inadmissible evidence cannot be admitted at trial automatically; to be admissible, the probative value of the evidence must substantially outweigh its prejudicial effect.[105] Nevertheless, the federal rules allow a qualified expert to freely rely on the findings of others—and the prior statements of others—to offer an inculpatory opinion in a court of law.

In effect, then, the special rules governing experts allow expert testimony to serve as a vehicle for accusatory out-of-court statements, which is the harm that the Confrontation Clause aims to prevent. This fact has not been ignored by litigants. With the increasing reliance on scientific evidence in criminal trials, many criminal defendants have successfully launched Confrontation Clause challenges to expert opinions based on otherwise inadmissible accusatory evidence.[106]

II. AI AND THE CONFRONTATION CLAUSE

AI in the courtroom will test the boundaries of the Confrontation Clause. As a threshold inquiry, this Part will first determine the extent to which AI-generated data can be testimonial hearsay for Confrontation Clause purposes. Specifically, this section will provide a preliminary analysis of the extent to which a forensic report generated by AI-enabled forensic machines can be "testimonial" and "hearsay" in a Confrontation Clause

[102] *See id.*

[103] FED. R. EVID. 701.

[104] FED. R. EVID. 703. Such inadmissible facts and data may be relied upon so long as "experts in the particular field would reasonably rely on [them]." *Id.*

[105] *See id.*

[106] *See, e.g.*, Bullcoming v. New Mexico, 564 U.S. 647, 651 (2011); United States v. Ignasiak, 667 F.3d 1217, 1230–33 (11th Cir. 2012); *see also infra* Section II.A.

analysis. Next, this Part will use a series of hypotheticals to illustrate the outer boundaries of this doctrine.

A. AI-Generated Data as "Testimonial" Evidence

To violate the Confrontation Clause, a statement must be "testimonial" and an "out-of-court statement offered for the truth of the matter asserted." To determine whether a statement is testimonial, courts apply the "primary purpose" test.[107] As a general matter, a statement will be "testimonial" if its primary purpose is to aid in a criminal prosecution.[108] Nevertheless, this definition would be an oversimplification of the primary purpose test as it has been construed by the courts. Unfortunately, the exact contours of the "primary purpose test" are blurry and inconsistently applied in practice.[109]

At least three different formulations of the test appear in the caselaw, and it is not clear which formulation a court should apply in a given case.[110] One approach focuses on the "evidentiary purpose" of the statement.[111] Under this formulation of the test, a statement is testimonial where "circumstances objectively indicat[ing] . . . that the primary purpose" of the statements was "to establish or prove past events potentially relevant to later criminal prosecution."[112] Other courts have applied an approach that emphasizes whether the statement serves as a "substitute" for testimony.[113] Under this approach, a statement

[107] *See, e.g.*, Ohio v. Clark, 576 U.S. 237, 244, (2015) (describing the "primary purpose test").

[108] *See Davis*, 547 U.S. at 822.

[109] *See* Christine Chambers Goodman, *Confrontation's Convolutions*, 47 LOY. U. CHI. L.J. 817, 849 (2016) (referring to the Confrontation Clause doctrine as "muddled").

[110] Disaggregating the primary purpose test into these approaches is supported by the analysis of Professors David H. Kaye, David E. Bernstein, Andrew Guthrie Ferguson, Maggie Wittlin and Jennifer L. Mnookin as it appears in THE NEW WIGMORE: A TREATISE ON EVIDENCE: EXPERT EVIDENCE § 5.3.2 (3d ed., 2023). To be sure, there are more skeptical interpretations of the inconsistencies in Confrontation Clause jurisprudence. Some scholarship has cast doubt on the proposition that there is a meaningful way to reconcile these doctrinal inconsistencies; some scholars have referred to confrontation jurisprudence as a "debacle," George Fisher, *The* Crawford *Debacle*, 113 MICH. L. REV. FIRST IMPRESSIONS 17, 24 (2014), and as "unworkable," David Crump, *Overruling Crawford v. Washington: Why and How*, 88 NOTRE DAME L. REV. 115, 137 (2012).

[111] *See Bullcoming*, 564 U.S. at 664; *Davis*, 547 U.S. at 822.

[112] *Davis*, 547 U.S. at 822; *see also Clark*, 576 U.S. at 244 ("[Statements] are testimonial when the circumstances objectively indicate that there is no such ongoing emergency, and that the primary purpose of the interrogation is to establish or prove past events potentially relevant to later criminal prosecution." (quoting *Davis*, 547 U.S. at 822)).

[113] *See, e.g.*, Michigan v. Bryant, 562 U.S. 344, 358 (2011).

is testimonial when it is "procured with a primary purpose of creating an out-of-court substitute for trial testimony."[114] Still yet, other courts have applied a "targeted accusation" test to determine if the statement is testimonial.[115] In these cases, a court will hold that a statement is testimonial if it has "the primary purpose of accusing a targeted individual of engaging in criminal conduct."[116] These variations of the primary purpose test complicate the confrontation analysis.[117]

Nevertheless, recent cases by the Supreme Court interpreting forensic laboratory reports may offer some guidance on how a court might apply the primary purpose test in cases involving an AI-generated forensic report. In *Melendez-Diaz v. Massachusetts*,[118] the Court concluded that toxicology certificates of analysis were testimonial.[119] These certificates had been prepared by analysts for the sole purpose of providing "'prima facie evidence of the composition, quality, and the net weight' of the analyzed substance" in the prosecution's case.[120] Echoing the "substitute testimony" approach delineated above, the court concluded that the certificates were "made under circumstances which would lead an objective witness reasonably to believe that the statement would be available for use at a later trial."[121] The Court noted that "[t]he 'certificates' are functionally identical to live, in-court testimony, doing 'precisely what a witness does on direct examination.'"[122]

---

[114] *Id.*

[115] *See, e.g.*, Williams v. Illinois, 567 U.S. 50, 82 (2012).

[116] *Id.*; State v. Michaels, 95 A.3d 648, 664 (N.J. 2014) (referring to *Williams*'s approach as the "targeted-accusation test"). *Williams* also seemed to suggest that the "formality" of the statement should weigh into the analysis. *See id.* (noting that, in past cases, testimonial statements typically "involved formalized statements such as affidavits, depositions, prior testimony, or confessions"). It is unclear how much this factor should weigh into the primary purpose inquiry. *See id.* at 138–39 (Kagan, J., dissenting) (criticizing an approach focused on formality).

[117] *Compare* Melendez-Diaz v. Massachusetts, 557 U.S. 305, 309–11 (2009) (applying a version of the "substitute testimony" approach and concluding that a forensic report was testimonial), *with* Williams, 567 U.S. at 82–84 (applying the "targeted accusation" approach and concluding that a forensic report was not testimonial).

[118] 557 U.S. 305 (2009).

[119] *Id.* at 310-11.

[120] *Id.* at 311 (citation omitted).

[121] *Id.* (internal quotation marks and citation omitted).

[122] *Id.* at 310–11 (citation omitted).

In *Bullcoming v. New Mexico*,[123] the Court arrived at the same outcome—the Court held that the forensic reports prepared by a lab analyst to "assist in police investigations" were testimonial.[124] This time, however, the Court seemed to adopt more of an "evidentiary purpose" approach to the primary purpose test.[125] The prosecution had argued that the analyst was not acting "adversarial[ly];" instead, the analyst was merely an "independent scientis[t]" making simple "observations."[126] The Court rejected that argument, holding that "[a] document created solely for an 'evidentiary purpose,' . . . [that is, a document] made in aid of a police investigation, ranks as testimonial."[127]

In *Williams v. Illinois*,[128] the Court applied the "targeted accusation" test and arrived at an entirely different result from *Melendez-Diaz* and *Bullcoming*.[129] There, the Court concluded that a forensic report prepared by a lab analyst for a police investigation was not testimonial.[130] The Court reasoned that the report was "not [made] to accuse petitioner."[131] Instead, the purpose of procuring the report was to "catch a dangerous [criminal] who was still at large."[132] The Court emphasized that "[t]he technicians who [conduct a laboratory test] generally have no way of knowing whether it will turn out to be incriminating or exonerating—or both."[133] Thus, there was a lack of a "targeted" accusatory purpose.[134]

---

[123] Bullcoming v. New Mexico, 564 U.S. 647, 651 (2011).

[124] *Id.* at 663–65.

[125] *See id.*

[126] *Id.* at 664 (citations omitted).

[127] *Id.* at 649 (citation omitted).

[128] 567 U.S. 50 (2012).

[129] *Id.* at 84.

[130] *Id.* at 84–86.

[131] *Id.* at 84. The Court also noted that the report was not "to create evidence for use at trial." *Id.* At first glance, this seems to be a reference to the "evidentiary purpose" approach. *See id.* at 121. But the rest of the analysis focuses on whether the statement had an accusatory effect. *See id.* at 85 ("[T]he primary effect of the profile is to exonerate a suspect who has been charged or is under investigation.").

[132] *Id.* at 84.

[133] *Id.* at 85.

[134] The facts of *Williams* differed from that of *Bullcoming* and *Melendez-Diaz* in one notable way. Namely, when the analysts in *Williams* ran their forensic tests, "[the defendant] had not yet been identified as a suspect." *Id.* at 85–86. Accordingly, there was a lack of knowledge by the analysts that they were aiding in a police investigation or a criminal prosecution of this particular defendant. *See id.* Nevertheless, the targeted-accusation test has been applied with the same result as *Williams* even in cases where a

These cases demonstrate the lack of certainty in determining whether an AI-generated test result would be "testimonial" under the "primary purpose test." The outcome depends largely on what test a court applies.[135] Should a court treat an AI-generated report analogously to a forensic report, *Melendez-Diaz*, *Bullcoming,* and *Williams* may inform the analysis. These cases provide an illustration of how a court would assess forensic reports through the application of variable approaches to the "primary purpose test."

B. AI-Generated Data as an Out-Of-Court "Statement"

To fall within the ambit of the protections of the Confrontation Clause, there must be an out-of-court statement offered to prove the truth of the matter asserted—meaning, there must be hearsay.[136] An expert repeating an operator's written statement for the truth of the matter asserted amounts to hearsay within the coverage of the Confrontation

---

defendant is already "known" and in custody. *See* Paredes v. State, 439 S.W.3d 522, 527 (Tex. App. 2014), *aff'd*, 462 S.W.3d 510 (Tex. Crim. App. 2015) (concluding that, in a case where a lab analyst conducted a test for the prosecution while a defendant was in custody, the report "was not prepared 'for the primary purpose of accusing' appellant" (quoting *Williams*, 567 U.S. at 83)); Washington v. Griffin, 142 F. Supp. 3d 291, 296 (E.D.N.Y. 2015), *aff'd*, 876 F.3d 395 (2d Cir. 2017) ("[W]hether the defendant was in custody was not the [*Williams*] plurality's only consideration for determining the primary purpose of the DNA profile; it also considered that '[w]hen 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 . . . .'"); State v. Norman, 125 P.3d 15, 19 (Or. App. 2005).

[135] *See* People v. Wakefield, 195 N.E.3d 19, 30–31, *reargument denied*, 192 N.E.3d 1152 (N.Y. 2022), *and cert. denied sub nom.* Wakefield v. New York, 143 S. Ct. 451 (2022), *reh'g denied*, No. 22-5588, 2023 WL 3046252 (U.S. Apr. 24, 2023) (concluding that a DNA report produced by a probabilistic genotyping model that used "some measure" of artificial intelligence was "testimonial" because [t]he report was prepared…at the request of the People for purposes of prosecuting defendant in a pending criminal proceeding."). This seems to be an application of the "evidentiary purpose" test. *See also* State v. Stillwell, 232 A.3d 363, 372 (N.H. 2019) (where the New Hampshire Supreme Court "conclude[d] that the machine-generated raw DNA profile data [from TrueAllele] . . . [was] not a testimonial statement." Adopting some version of the "targeted accusation" approach, the court emphasized that the technicians operating the software had no way of knowing what result the raw machine readouts would yield. *See id.* at 602–03 (noting that a lab technician could not "independently affirm or deny that a blood sample contain[ed] a particular characteristic," since he would merely be relying on the machine's printouts)). *Stillwell* can also be framed as an application of the machine-generated data exception to confrontation, which is discussed in detail in the below section. *See infra* Part II.B.

[136] *Crawford*, 541 U.S. at 53, 59.

Clause.[137] But the case law becomes less clear when an expert recites the raw results produced by a forensic machine. In some cases, courts treat such "statements" as "raw data," analogous to physical evidence.[138] Courts have deemed this "raw data" to be a conveyance of the forensic machine.[139] But a machine cannot be a declarant.[140] It also cannot be "a 'witness against' anyone."[141] Thus, courts conclude that a forensic machine's printout of raw data is not covered by the Confrontation Clause.

The delineation between "machine-generated data" and a "human" statement is the application of human expertise. The test results of a forensic machine will only be considered a statement of the machine if those results are generated by a sufficiently automated mechanized process.[142] A sufficiently automated mechanized process is a process in which human intervention is effectively absent.[143] This is not an absolute bar on human involvement.[144] As the Eleventh Circuit noted in *United States v. Lamons*,[145] "there can be no statements which are wholly machine-generated in the strictest sense; all

[137] *See, e.g.*, United States v. Blazier, 69 M.J. 218, 226 (C.A.A.F. 2010) ("An expert witness may review and rely upon inadmissible hearsay in forming independent conclusions, but he may not circumvent . . . the Sixth Amendment by repeating the substance of the hearsay.").

[138] *See* United States v. Washington, 498 F.3d 225, 230 (4th Cir. 2007); United States v. Lamons, 532 F.3d 1251, 1265 (11th Cir. 2008); United States v. Moon, 512 F.3d 359, 362 (7th Cir. 2008); United States v. Summers, 666 F.3d 192, 202 (4th Cir. 2011); United States v. Lizarraga-Tirado, 789 F.3d 1107, 1110 (9th Cir. 2015); United States v. Miller, 982 F.3d 412, 437 (6th Cir. 2020); United States v. Arce, 49 F.4th 382, 392 (4th Cir. 2022).

[139] *Washington*, 498 F.3d at 230.

[140] *See id.*

[141] *Moon*, 512 F.3d at 362 ("If the readings are 'statements' by a 'witness against' the defendants, then the machine must be the declarant. Yet how could one cross-examine a gas chromatograph? Producing spectrographs, ovens, and centrifuges in court would serve no one's interests.").

[142] *See Washington*, 498 F.3d at 231; *Lamons*, 532 F.3d at 1263–64; *Lizarraga-Tirado*, 789 F.3d at 1110.

[143] *See Washington*, 498 F.3d at 231; *Lamons*, 532 F.3d at 1263–64 ("We have no difficulty concluding that the statements in question are the statements of machines . . . the relevant point is that no human intervened at the time the raw billing data was 'stated' by the machine . . . ."); *Lizarraga-Tirado*, 789 F.3d at 1110 (concluding that Google Earth was not a hearsay declarant and noting that "[t]he program analyzes the GPS coordinates and, without any human intervention, places a labeled tack on the satellite image."); *see also* People v. Holowko, 486 N.E.2d 877, 879 (Ill. 1985) ("[C]omputer-generated data are different. The evidence is generated instantaneously as the telephone call is placed, without the assistance, observations, or reports from or by a human declarant.").

[144] *Lamons*, 532 F.3d at 1263 n.23.

[145] *Id.*

machines were designed and built by humans."[146] Nevertheless, "certain statements involve so little intervention by humans in their generation as to leave no doubt that they are wholly machine-generated for all practical purposes."[147]

The degree of human intervention necessary to convert a machine-generated printout into the "statement" of a human operator is difficult to pinpoint in the caselaw. But the caselaw makes clear that where an operator is merely inputting a sample into a machine to produce an output, without further interpretation or analysis, that degree of human intervention is insufficient.[148] To illustrate, consider the Fourth Circuit's decision in *United States v. Washington*.[149] There, the court concluded that a gas chromograph's toxicology results amounted to "machine-generated information" sufficiently lacking in human intervention.[150] The Court rejected the argument that an inculpatory toxicology report generated by the machine was the "statement" of the lab technicians who operated the machine.[151] Instead, the court concluded that "the inculpating 'statement'"—the toxicology report—"was made by the machine on printed sheets."[152] The court reasoned that "[t]he machines generated data by manipulating blood through a common scientific and technological process."[153] On the other hand, "[t]he lab technicians' role was simply to operate the machines," which did not amount to sufficient human intervention.[154]

The court noted the significance of the fact that the diagnostic machine only permitted the operators to input data for analysis; the machine did not allow the operators to convey a communicative assertion through it. As the court put it, "the chromatograph machine's output is a mechanical response to the item analyzed and in no way is a communication of the operator."[155] In contrast to "a typewriter or telephone," which "transmits the communicative assertion of the operator, the chromatograph [diagnostic] machine transmits data it derives from the sample being analyzed, independent of what

[146] *Id.*
[147] *Id.*
[148] *See Washington*, 498 F.3d at 230 & n.2; *See also Moon*, 512 F.3d at 362.
[149] 498 F.3d 225 (4th Cir. 2007).
[150] *Id.* at 228, 230–32.
[151] *Id.* at 230.
[152] *Id.*
[153] *Id.*
[154] *Id.*
[155] *Id.* at 235 n.2.

the operator would say about the sample, if he or she had anything to say about it."[156] Thus, the court "reject[ed] the characterization of the raw data generated by the lab's machines as statements of the lab technicians who operated the machines."[157] Instead, the court concluded that "[t]he raw data generated by the diagnostic machines are the 'statements' *of the machines* themselves, not their operators."[158]

Nevertheless, if an operator were to subject a machine-generated output to human analysis and record a conclusion based on that output, that resulting report would be an "assertion" of the human operator, even if the report contained recitations of the "raw data."[159] The Eleventh Circuit's decision in *United States v. Ignasiak*[160] is instructive.[161] There, a toxicology report had been generated by a diagnostic machine—just like in *Washington*.[162] The critical difference, however, was that the medical examiners had interpreted that report and used it to draw a conclusion as to the cause of death of a victim.[163] The examiners then recorded their findings in an autopsy report, which contained the toxicology report.[164]

The court emphasized the fact that the autopsy report contained more than just the toxicology results; rather, the medical examiners had added their human analysis to arrive at an independent judgment. As the court put it, the report was "replete with the extensive presence and intervention of human hands and exercise of judgment," including recorded "observations and impressions" of the decedent, as well as a diagnosis as to the cause of death—accidental overdose.[165] Thus, the court concluded that "there [was] little, if any, raw data or conclusions reflected in [the] autopsy report—aside from the results of toxicology testing—that is not dependent upon the skill, methodology and judgment

[156] *Id.*
[157] *Id.* at 230 (emphasis omitted).
[158] *Id.* at 230 (emphasis in original).
[159] *Moon*, 512 F.3d at 362 ("The physician's diagnosis is testimonial, but the lab's raw results are not, because data are not 'statements' in any useful sense."); *see also* United States v. Ignasiak, 667 F.3d 1217, 1230–33 (11th Cir. 2012).
[160] 667 F.3d 1217 (11th Cir. 2012).
[161] *See id.* at 1229–37.
[162] *Id.* at 1225–26, 1233.
[163] *Id.* at 1231–33.
[164] *Id.*
[165] *See id.*

exercised by the actual medical examiner who performed the autopsy."[166] Accordingly, the "[m]edical examiners [were] not mere scriveners reporting machine generated raw-data."[167]

Washington and *Ignasiak* illustrate that, so long as a forensic analyst merely inputs the sample into a machine and lets the machine render the analysis, the resulting printout will be the "statement" of the machine. Meaning, it will be "raw data," analogous to physical evidence, which is not covered by the protections of the Confrontation Clause. This reasoning has been applied in many cases, involving varying types of forensic technology, including breath readers,[168] gas chromatographs,[169] infrared spectrometers,[170] DNA typing,[171] and automatically labeled GPS coordinates.[172] To be sure, there has been some resistance to the machine-generated data exception, but *Washington*'s analysis seems to be the majority approach.[173]

---

[166] *Id.* at 1233.

[167] *Id.* at 1232.

[168] *See* Wimbish v. Commonwealth, 658 S.E.2d 715, 719 (Va. Ct. App. 2008) ("The Intoxilyzer 5000 . . . is not a witness or declarant capable of making statements."); State v. Buckland, 313 Conn. 205, 221, 96 A.3d 1163, 1172 (2014) (applying exception to Draeger machine reports); Cranston v. State, 936 N.E.2d 342, 344 (Ind. Ct. App. 2010) (applying exception to Datamaster evidence tickets); People v. Dinardo, 290 Mich. App. 280, 291, 801 N.W.2d 73, 79 (2010) (applying exception to Datamaster evidence tickets).

[169] *Moon*, 512 F.3d at 361–64; *see also* State v. Michaels, 219 N.J. 1, 44, 95 A.3d 648, 675 (2014) ("Clearly, defendant could not cross-examine the [chromatography/mass spectrometry] machines themselves."); United States v. Turner, 591 F.3d 928, 932 (7th Cir. 2010), *cert. granted, judgment vacated*, 567 U.S. 947, 133 S. Ct. 55, 183 L. Ed. 2d 698 (2012) ("We also held that instrument readouts were not 'statements' . . . .").

[170] *See Moon*, 512 F.3d at 361–64.

[171] United States v. Summers, 666 F.3d 192, 202 (4th Cir. 2011) ("The numerical identifiers of the DNA allele here, insofar as they are nothing more than raw data produced by a machine, are indistinguishable in character from the gas chromatograph data in *Washington* and the chromatograph and spectrometer results in *Moon* and *Turner*.").

[172] *Lizarraga-Tirado*, 789 F.3d at 1109–10 ("A tack placed by the Google Earth program and automatically labeled with GPS coordinates isn't hearsay."); United States v. Nelson, 533 F. Supp. 3d 779, 801 (N.D. Cal. 2021); *see also* City of LaVergne v. Gure, No. M202000148COAR3CV, 2022 WL 3709387, at *3 (Tenn. Ct. App. Aug. 29, 2022) ("Google Maps is not a person. So it is not a 'declarant.'").

[173] For instance, in his dissent in *Washington*, Circuit Judge M. Blane Michael would have held that "the test results are the hearsay statements of the laboratory technicians." *See Washington*, 498 F.3d at 232 (Michael, J., dissenting). Judge Michael emphasized that there is "only one circumstance" where "a computer-generated assertion [is] not considered the statement of a person: when the assertion is produced without *any* human assistance or input." *Id.* at 233 (emphasis added). And in *Washington*, the "computerized laboratory equipment" could not have "detect[ed], measure[d], and record[ed] toxin levels

Under the majority approach, AI-generated statements would likely be treated as "machine-generated raw data." As a general matter, an AI model is likely a sufficiently "automated" or "mechanistic" process to fall within the "machine-generated data" exception. An AI system limits human intervention by design.[174] To illustrate, in the machine learning context, the purpose of the "learning" process is to train the algorithm to identify patterns without overwhelming human intervention.[175] The algorithm sorts through more data than any human could.[176]

To be sure, some human intervention is required—an analyst must input data into the model. But merely inputting data into the model is insufficient to convert AI-generated data into a "statement" of the model's operator. *Washington* and its progeny stand for the proposition that merely inputting a sample into a machine, without further analysis by the operator, will not rise to the level of human intervention needed to convert the machine conveyance into a "communicative assertion."[177] Like the lab operators in *Washington*, the AI model's operators are merely inputting data into a "machine" and producing a result.[178]

Further, like the diagnostic machine in *Washington*, an AI model used for forensic testing would not permit an operator to convey a "communicative assertion" through it. Instead, "the [AI model]'s output is a mechanical response to the item analyzed and in no way is a communication of the operator."[179] Unlike a typewriter or a telephone, the AI model

---

in blood samples without the assistance or input of a trained laboratory technician." *See id.* The D.C. Court of Appeals seemed to adopt Judge Michael's more stringent approach to machine statements in *Young v. U.S.*, 63 A.3d 1033 (D.C. 2013). There, the court concluded that "it [was] too simplistic to say the DNA profiles and the RMP [random match probability] printout were not hearsay because they were 'nothing more than raw data produced by a machine.'" *Id.* 1045–50. Instead, the Court reasoned that "the DNA profiles and, perhaps, the . . . printout [from the DNA typing software], do not stand on their own but, instead, have meaning because they amount to a communication by the scientists who produced them." *Id.* at 1046. That assertion was, "essentially, that the scientists generated these specific results by properly performing certain tests and procedures on particular, uncorrupted evidence and correctly recording the outcomes." *Id.*

[174] *See* Surden, *Artificial Intelligence and Law*, *supra* note 33, at 1307.

[175] *See* Surden, *Machine Learning and Law*, *supra* note 37, at 89–90.

[176] *See id.* at 89–90, 94–95; *see also* Erickson et al., *supra* note 39, at 505–06.

[177] *Washington*, 498 F.3d at 230–32.

[178] *See id.*

[179] *Id.* at 230 n.2.

"transmits data it derives from the sample being analyzed, independent of what the operator would say about the sample."[180] Thus, the raw data generated by the model are "'statements' of the machine[] . . . not [its] operators."[181]

To be sure, if the operators added to this raw data by drawing on their human expertise to form an independent judgment, the resulting statement would be that of the operators rather than the machine. Put another way, if an operator conducted a review of the raw data by applying human "skill, methodology and judgment," and then detailed an analytical conclusion in a report, that report would not be considered "machine generated."[182] Instead, that statement would be analogous to the autopsy report in *Ignasiak*.[183] Such a statement would be "replete with the extensive presence and intervention of human hands and exercise of judgment."[184] But in the absence of modification by human intervention, the raw test results of the machine learning algorithm would amount to "machine-generated" raw data.[185]

It is worth noting that this analysis operates under the assumption that courts will apply existing legal doctrines to AI—but it is entirely possible that constitutional standards will shift in cases involving AI simply because AI is different. AI models are unique from other more traditional technologies in that their capabilities, by definition, mirror many of the cognitive capacities of a human. In many respects, a highly sophisticated AI-enabled forensic machine can effectively serve the role of a human forensic analyst.[186] As one court put it, "in the brave new world of artificial intelligence, the finger of accusation is often pointed, not by a human being, but by an algorithm."[187]

In *People v. Wakefield*,[188] the New York Supreme Court, Appellate Division, Third Department, lent some support to this idea of "AI exceptionalism," albeit in dicta.[189] There, the court noted that, "[g]iven the exponential growth of technologies such as

[180] *Id.*
[181] *Id.* at 230.
[182] *Ignasiak*, F.3d at 1232–33.
[183] *Id.* at 1229–37.
[184] *Id.* at 1233.
[185] *See Washington*, 498 F.3d at 230–32.
[186] *See* R.L.G. v. State, 322 So. 3d 721, 725 (Fla. Dist. Ct. App. 2021).
[187] *Id.*
[188] 175 A.D.3d 158 (N.Y. App. Div. 2019), *aff'd*, 195 N.E.3d 19 (N.Y. 2022).
[189] *See id.* at 165, 169. TrueAllele uses "a certain degree of artificial intelligence." *Id.* at 162.

artificial intelligence, to embrace the future we must assess, and perhaps reassess, the constitutional requirements of due process that arise where law and modern science collide."[190] Although the court rejected the defendant's argument that a probabilistic genotyping model's source code could be a "declarant" for Confrontation Clause purposes, the court declined to hold that "an artificial intelligence-type system could *never* be a declarant."[191]

Nevertheless, under current law, it seems likely that an AI-generated printout would be treated as raw data. Such a printout would not be a "statement." Accordingly, its introduction by an expert would not amount to hearsay, meaning that it falls outside of the protection of the Confrontation Clause.

C. Hypotheticals

Conceptualizing the limits of Confrontation Clause jurisprudence is difficult because of how fact-dependent these analyses can be. Due to this doctrine's context-specific nature, this section provides a series of illustrative hypotheticals to demonstrate the outer boundaries of the Confrontation Clause in cases involving AI-generated forensic readouts. These hypotheticals are variations of the facts of real-world cases, which are detailed in the footnotes below.

1. Confronting the Absent Technician

An expert witness ("Expert") is testifying on behalf of the prosecution in a criminal trial. Expert is a duly qualified expert in machine learning applications in voice recognition. Expert introduces a printout generated by AI—namely, a probabilistic model used for voice recognition. The printout reads that, with a 98% random match probability, the voice fingerprint collected from the crime scene matches the profile of the defendant ("Defendant") in the FBI's voice-fingerprinting database. Expert did not personally upload or analyze the collected voice fingerprint sample. Instead, a forensic technician operated the model and generated the result, while the model analyzed the collected voice fingerprint sample. Defendant wishes to call the technician to the stand to ensure the test was run, and that the data was uploaded properly.

---

[190] *Id.* at 165.

[191] *Id.* at 169 (emphasis added); People v. H.K., 69 Misc. 3d 774, 785 (N.Y. Crim. Ct. 2020) (distinguishing between an AI-enabled probabilistic genotyping model and a more traditional model and referring to the latter as a "highly sophisticated calculator").

Defendant has no right to confront the technician who merely operated the model. As a preliminary matter, under the "primary purpose test," it is unclear if such a printout is "testimonial."[192] If the "substitute testimony" or "evidentiary purpose" approaches are applied, the printout would likely be testimonial since it was procured by the technician to be presented in court to prove past events relevant to the prosecution's case.[193] On the other hand, if the "targeted accusation" test is applied, a court might conclude that there was no certainty the statement was intended to be accusatory.[194] Like in *Williams v. Illinois*, "[t]he technicians who [conduct the test] generally have no way of knowing whether it will turn out to be incriminating or exonerating."[195]

Irrespective of whether the printout passes the primary purpose test, however, it will very likely fail under the second prong of the analysis—whether it is an out-of-court statement. The machine-generated printout would likely fall under the machine-generated data exception for hearsay.[196] The technician's only role was to input the data into the model, while the model analyzed the data and generated the result. Although there is certainly human involvement in the generation of the data in that it is inputted into a program created by human developers, this level of human intervention has been deemed insufficient by many courts.[197] Thus, the machine-generated data exception applies, and the printout is treated as a statement of the model. Accordingly, Defendant has no right to confront the operator.

2. Confronting the Absent Developer

Expert testifies for the prosecution in a criminal trial. Expert is a duly qualified expert in deep learning applications for probabilistic genotyping. Expert introduces a printout generated by AI—namely, a model used for DNA genotyping. The printout reads that, with a 98% random match probability, the DNA profile collected from the crime scene matches Defendant's profile in CODIS. Expert analyzed the DNA sample and inputted it into the model. Nevertheless, Expert did not design the model, write its source code, or

[192] *See supra* Section II.A.
[193] *See Davis*, 547 U.S. at 822; *Michigan*, 562 U.S. at 358.
[194] *See Williams*, 567 U.S. at 85.
[195] *See id.*
[196] *See Washington*, 498 F.3d at 230; *Lamons*, 532 F.3d at 1265; *Lizarraga-Tirado*, 789 F.3d at 1110.
[197] *See, e.g., Washington*, 498 F.3d at 230.

play any role in its development. Defendant wishes to call the absent developer to the stand for cross-examination.

As in the above hypothetical, under the "primary purpose test," it is unclear if such a printout is testimonial. This will depend largely on the test a court chooses to apply. In any case, the machine-generated data exception would likely bar any claim that the printout is a "statement" of the developer. Just as a technician does not convey a communicative assertion through an AI model by inputting data, a developer does not convey a communicative assertion through an AI model by drafting its source code.[198] As the Sixth Circuit noted in *United States v. Miller*,[199] "[t]he Confrontation Clause does not give [the defendant] a right to cross-examine the individuals who created [a computer's] systems."[200] In *State v. Linder*,[201] the Arizona Court of Appeals reached the same result as *Miller*: "[i]t is . . . not necessary . . . for the creator of the device's source code to produce that code and appear for cross-examination at trial."[202]

3. Confronting the AI Model

Expert testifies for the prosecution in a criminal trial. Expert is a duly qualified expert in machine learning applications in global positioning systems. Expert introduces a printout generated by an AI system—here, a machine learning model used for gunshot location. The printout reads that, with 98% certainty, the gunfire originated from Defendant's location. Expert collected the data from the scene, inputted the data into the model, and recorded the result. Defendant wishes to review the source code of the model to test its reliability, but the source code is trade secret protected. Defendant raises a Confrontation Clause challenge.

The Confrontation Clause, at least as it is currently interpreted, will likely not provide any relief to Defendant. The right to confrontation applies only to human witnesses.[203] Courts have repeatedly rejected the proposition that a model's "source code" can be

[198] *See Washington*, 498 F.3d at 230; *Lamons*, 532 F.3d at 1265; *Lizarraga-Tirado*, 789 F.3d at 1110.

[199] 982 F.3d 412 (6th Cir. 2020)

[200] *Id.* at 435–36, 438 (applying this rationale to certain readings from a CyberTipLine Report); *id.* (noting that the "[computer] systems automatically performed [its functions] . . . [a]nd they automatically recorded the results (or 'statements')").

[201] 252 P.3d 1033 (Ariz. Ct. App. 2010).

[202] *Id.* at 1036 (applying this rationale to the readings from an Intoxilyzer breathalyzer).

[203] *Moon*, 512 F.3d at 362.

"called" into court through a confrontation challenge.[204] As the New York Court of Appeals put it in *People v. Wakefield*, "the source code is not an entity that can be cross-examined."[205] To be sure, it is entirely possible that a highly sophisticated AI might alter this proposition. Nevertheless, the current approach does not appear to carve out a doctrinal exception for AI.[206]

III. IMPLICATIONS AND RECOMMENDATIONS

This Paper has revealed that, in a world where courtrooms are dominated by AI-generated data, the Confrontation Clause's protections will become increasingly eroded. This is significant for two reasons. First, as a practical matter, these limitations may impede a criminal defendant's ability to test the reliability of inculpatory statements generated by AI models in court. Second, as a normative matter, these limitations are concerning for the future of the right to confrontation, which is a constitutional guarantee designed "to ensure reliability of evidence."[207]

A. Practical Implications

Measuring the practical effects of these rights limitations is a difficult task, but there is some evidence that these limitations could have a measurable impact on a defendant's ability to test the reliability of an AI model in court. To illustrate, an inability to confront the model's developer seems like a significant loss for the defendant. Presumably, this is the person with the most knowledge of the inner workings of the model. Even then, however, there are limits to this right's utility: even the algorithm's creator may not have full knowledge of the model's inner processes, which may be as inscrutable as they are unexplainable.[208] Nevertheless, there are certainly some valuable questions a defendant

[204] *See, e.g.*, *Wakefield*, 195 N.E.3d at 31 ("[W]e reject defendant's novel argument that the source code is the declarant. Even if the TrueAllele system is programmed to have some measure of 'artificial intelligence,' the source code is not an entity that can be cross-examined."); People v. Perez, No. A165848, 2022 WL 17985920, at *16 (Cal. Ct. App. Dec. 29, 2022), *review denied* (Mar. 15, 2023).

[205] *Wakefield*, 195 N.E.3d at 31.

[206] *Id.* at 31; *Perez*, 2022 WL 17985920, at *16.

[207] *Crawford*, 541 U.S. at 61.

[208] It is also worth noting that a robust right to "call the developer" could have problematic policy implications. This right must be balanced against the practical problem of potentially requiring developers to be hailed to court in every case where their algorithm is used.

could ask on cross-examination, including inquiries relating to optimization and validation testing.[209]

An inability to confront the technician or analyst who operated the model could also hinder a defendant's ability to build his or her case. While it is true that the operator—who merely inputted the data—may have limited knowledge of the internal processes of the model, there is still some value to cross-examination for reliability testing. To illustrate, cross-examination could provide a defendant with an opportunity to test for malfeasance, lack of truthfulness, or to simply ensure the forensic test was actually run.[210] At a minimum, this right would provide a defendant with one additional chance to mount a defense, which could very well make a difference in close cases.

An inability to "confront the source code" is perhaps the least detrimental loss for defendants in a future where AI dominates criminal prosecutions. This is because source code is difficult to scrutinize and review. To illustrate, the source code at issue in *Wakefield* had nearly 170,000 lines of code.[211] Reviewing that source code at ten lines of code an hour would take around 8.5 years to complete.[212] Nevertheless, there is still some value to obtaining source code and reviewing it for errors—but only if criminal defendants have adequate expertise and resources to effectively test its reliability. Thus, there is arguably some value lost due to these limitations to the right to confrontation.

This analysis, however, leaves out the fact that testing by cross-examination is not the only means to test the reliability of evidence in court. Other means of ensuring reliability include authentication under Rule 901 and admissibility under the *Daubert* standard for

[209] *See infra* Part III.B.

[210] While there is no guarantee that an analyst will tell the truth, there is some value to the idea that an analyst would need to testify under oath in a court of law. *See* Nadine Farid, *Oath and Affirmation in the Court: Thoughts on the Power of a Sworn Promise*, 40 NEW ENG. L. REV. 555, 557 (2006) ("[T]hat the oath implicates the motivations it does, that it is in fact so compelling, is indicative of its distinctive stature in our legal system. Nothing, it seems, is as effective in helping to ascertain the truth in the courtroom.").

[211] Lauren Kichner, *Powerful DNA Software Used in Hundreds of Criminal Cases Faces New Scrutiny*, THE MARKUP (Mar. 9, 2022, 8:00 AM), https://themarkup.org/news/2021/03/09/powerful-dna-software-used-in-hundreds-of-criminal-cases-faces-new-scrutiny [https://perma.cc/76UE-67JT].

[212] *Id.*

expert testimony.[213] If these rights are sufficient to ensure the reliability of evidence, perhaps the erosion of the right to confrontation does not mean much in practice for criminal defendants. *Ex ante* judicial gatekeeping will provide defendants with the means of probing the accuracy of the AI witnesses against them.

Unfortunately, there is some doubt that the standards governing authentication and expert testimony are sufficient in ensuring adequate reliability testing. Many scholars have pointed out the limits of these safeguards, particularly in cases involving process-based mechanistic or automatic evidence.[214] Authentication generally focuses on ensuring "that the item is what the proponent claims it is."[215] The rules provide several non-exclusive means of authentication, including Rule 901(b)(9), which governs in most cases involving computerized or digital evidence.[216] Rule 901(b)(9) provides that "[e]vidence describing a process or system [must] show[] that it produces an accurate result."[217] While the plain language of this rule seems to require stringent reliability testing, courts diverge in applying this rule.[218] Some courts have imported more stringent requirements into the test, while others have construed the rule more liberally.[219] The rules of evidence place the discretionary power of evidentiary gatekeeping in the court.[220] Regardless of the approach a judge takes, the burden of proof for authentication is remarkably low. The standard for authentication is a "mere preponderance"— "a relatively low threshold—51%, or slightly better than a coin toss."[221]

---

[213] *See* FED R. EVID. 901; Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 582 (1993); FED. R. EVID. 702.

[214] *See, e.g.*, Andrea Roth, *Machine Testimony*, *supra* note 27, at 2030–35; Hilbert, *supra* note 27, at 763.

[215] FED. R. EVID. 901(a).

[216] *See* FED R. EVID. 901(b)(9).

[217] *Id.*

[218] *See* Roth, *Machine Testimony*, *supra* note 27, at 2012–13 & 2013 n.200.

[219] *See id.* at 2012–13 ("For computerized business records, the authentication requirement of Rule 901(b)(9) may screen clearly unreliable processes, although . . . such records—like all machine conveyances—should also be open to impeachment and other scrutiny that provides the factfinder with additional context."); *id.* at 2013 n.200 (pointing out that "[s]ome courts, after *Daubert*, have interpreted Rule 901(b)(9) as a requirement that the opinions of computer simulations be 'reliable,' thus applying the *Daubert* requirements for human expert testimony to computer 'expert[s]'" (citation omitted)); *see also* Grimm et al., *supra* note 15, at 94 (calling on judges to scrutinize AI models under Rule 901 in cases where there is a "great[] . . . risk of unacceptable adverse consequences). *Cf. id.* at 95 (asserting that judges should "borrow" concepts from Rule 702, the rule governing expert evidence, to authenticate AI evidence).

[220] *See* Grimm et al., *supra* note 15, at 98.

[221] *Id.* at 94.

The *Daubert* standard for admitting expert testimony has been criticized for similar reasons. The rules governing expert witnesses require, among other things, that the expert is adequately qualified, that "the testimony is based on sufficient facts or data," that "the testimony is the product of reliable principles and methods," and that "the expert has reliably applied the principles and methods to the facts of the case."[222] Again, like the rules governing authentication, a plain reading of these factors seems to suggest that expert opinions require strict reliability testing. But, particularly in cases involving more complex systems and computational models, the standard is not applied consistently and with adequate rigor.[223] As one scholar pointed out, some "courts have admitted . . . nonscientific algorithms with no *Daubert* scrutiny at all."[224] And like the rules governing authentication, the *Daubert* standard is a mere preponderance.[225]

Still yet, these rules are further limited in that they can be skirted by a judge's decision to take judicial notice of a method or process under Rule 201.[226] Some judges have been quite liberal in exercising this power when it comes to evidence generated by algorithms.[227] To illustrate, in one recent case, a federal court took judicial notice of a Wikipedia entry.[228] This has led some scholars to criticize the relative ease by which courts are taking judicial notice of digital evidence and assert that judicial restraint under Rule 201 is needed.[229]

---

[222] FED. R. EVID. 702.

[223] Roth, *Machine Testimony*, *supra* note 27, at 2030–35 (describing reliability requirements for admissibility as it applies to mechanical and automatic evidence, including complex algorithms); Hilbert, *supra* note 27, at 763 (discussing, among other things, "*Daubert*'s limited impact on the criminal justice system, highlighting a few profoundly disturbing examples of unreliable forensic science that currently plague criminal courts").

[224] Roth, *Machine Testimony*, *supra* note 27, at 2014 (citing UMG Recordings, Inc. v. Lindor, 531 F. Supp. 2d 453, 457 (E.D.N.Y. 2007)).

[225] *See Daubert*, 509 U.S. at 593 (noting that "[t]hese matters should be established by a preponderance of proof," pursuant to Rule 104(a)); *see also* FED. R. EVID 104(a).

[226] *See* FED R. EVID. 201.

[227] *See* Bellin & Ferguson, *supra* note 26, at 1137–43.

[228] AVS Found. v. Eugene Berry Enter., LLC, No. 11 CV 01084, 2011 WL 6056903, at *6 (W.D. Pa. Dec. 6, 2011) (taking judicial notice of a Wikipedia entry for the Pittsburgh Steeler's "Terrible Towel®"); Kemp v. Zavaras, No. CIVA09CV00295WYDMJW, 2010 WL 1268094, at *2 n.3 (D. Colo. Mar. 29, 2010) (noting that a court can take judicial notice of distances between two points "using mapping services, such as Google Maps"); *see also* Bellin & Ferguson, *supra* note 26, at 1157–64 (collecting cases involving judicial notice of, among other things, "the MayoClinic website, stock prices reflected in Yahoo! Finance . . . and information contained in online flight schedules").

[229] Bellin & Ferguson, *supra* note 27, at 1137–43.

With this backdrop in mind, it is notable that the Confrontation Clause provides little protection to criminal defendants seeking to test the reliability of an AI model in court. While there are certainly other means of testing reliability other than cross-examination, many scholars have asserted that these alternative methods fail defendants in cases involving mechanistic and computational evidence.

B. Normative Implications

The normative implications of this analysis are as far-reaching as they are concerning. This case study provides an example of a constitutional right that is seemingly losing its utility in the modern age. In a future where AI-enabled forensic tools dominate criminal prosecutions, the scope of a defendant's right to confront witnesses via cross-examination will be increasingly diminished. Even if a broader right to confrontation is provided, cross-examination may not even be the best use of a defendant's time in building a defense.[230] The inner workings of many AI models are inscrutable, opaque, and difficult to convey to a jury through cross-examination.[231]

The dwindling reach and relevance of a right to confrontation is particularly concerning considering that the goal of confrontation is to ensure that evidence is reliable. As the Supreme Court emphasized in *Crawford,* "the Clause's ultimate goal is to ensure reliability of evidence."[232] Yet, *Crawford* and its progeny carefully framed the right as a "procedural guarantee" rather than a "substantive" one.[233] And that procedural guarantee is "particular"—it is a guarantee of the right to test reliability through "the crucible of *cross-examination.*"[234] As this study makes clear, the Court's decision to frame the right to confrontation in this way has far-reaching effects on its scope of application.

If the Confrontation Clause is really about "ensur[ing] reliability" of evidence, perhaps it should be refashioned to ensure that it provides that broad guarantee in the modern age. As the New York Supreme Court, Appellate Division, Third Department, noted in *Wakefield*, "[g]iven the exponential growth of technologies such as artificial intelligence, to embrace the future we must assess, and perhaps reassess, the constitutional requirements

[230] *See* Cheng & Nunn, *supra* note 27, at 1080, 1090.
[231] *See* Grimm et al., *supra* note 15, at 29–30, 60–65.
[232] *Crawford*, 541 U.S. at 61.
[233] *See id.*
[234] *Id.*

of due process that arise where law and modern science collide."[235] This study lends some support to the proposition that the right to confrontation should be reinterpreted to better align with the realities of technological progress.

This study illustrates how evidence law's focus on human witnesses can hamper litigants' abilities to adequately ensure the reliability of computational evidence. The Confrontation Clause's guarantee is "human-centric" in nature. Confrontation provides a right to cross-examination of *human* witnesses. Further, to prove a violation of the right to confrontation, there needs to be sufficient intervention from a human witness. Namely, a constitutional violation will only occur if there is a human declarant, a human statement, and a human assertion.[236] Whether a statement is testimonial requires an objective analysis of the human declarant's "primary purpose" in generating the statement. As this study has illustrated, it is precisely the "human-centric" aspects of the right to confrontation—the hearsay rule and the primary purpose test—that ultimately limit the scope of its constitutional safeguards.

Accordingly, this Paper lends support to a broader point about the law of evidence—perhaps the rules of evidence are overly focused on witness-based or human-centric evidence, to the detriment of "process-based" evidence.[237] As Professors Edward K. Cheng and G. Alexander Nunn point out, in many ways, the laws of evidence are exceedingly "focused on—or perhaps obsessed over—witnesses."[238] The rules governing experts focus on the human witness's qualifications, bases, and methods.[239] Similarly, the framework for admitting physical evidence operates through the conduit of human witnesses.[240] But when it comes to process-based evidence, such as mechanistic or automatic evidence, the rules of evidence are flustered.[241] As Cheng and Nunn assert, "[t]he traditional [witness-based scheme of evidence] hampers the use of process evidence, distorts its presentation, and fails to ensure its reliability."[242] The intersection of AI and the right to confrontation thus

[235] *Wakefield*, 175 A.D.3d at 165.
[236] *See id.* at 50–56.
[237] Cheng & Nunn, *supra* note 27, 1077–80.
[238] *See id.*
[239] *See id.* at 1077.
[240] *See id.*
[241] *Id.* at 1079–80.
[242] *Id.* at 1079–80.

provides yet another illustration of the limits of an exceedingly witness-centric approach to evidence law.

C. Planning for the Future

This study has highlighted some of the shortcomings of the reach of the right to confrontation in a world where AI dominates criminal prosecutions. But in undertaking this analysis, this Paper has had to make many predictions about the state of criminal adjudications in the near future. There are limitations to this analysis in that there is no way to empirically assess the extent to which a lack of access to confrontation in the future will harm criminal defendants. Nevertheless, this study has illustrated some notable loopholes in the right to confrontation as it intersects with AI in the courtroom. To ensure criminal defendants are afforded appropriate protections, this Paper makes the following recommendations to scholars and practitioners.

In the short-term, working from within the current regime of evidentiary rules can still ensure that the "ultimate goal" of confrontation—to ensure reliability—is met. A plain reading of the rules governing authentication and *Daubert* seems to provide for substantial safeguards for reliability testing.[243] However, scholars have criticized the inconsistency of these rules as they are applied in practice, as well as the tendency for judges to take judicial notice of digital evidence.[244] Providing judges with adequate resources to assist with evidentiary review of AI evidence and raising awareness about many of the pitfalls of AI-generated evidence may ensure that judges are well-prepared for its admission in practice. On the other hand, raising awareness about the importance of reliability testing in AI may not be the most effective in ensuring reliability. Judges still retain broad discretion in their gatekeeping role. But this could be a good starting point for longer term solutions.

In the longer term, courts might consider refining, reinterpreting, or restructuring evidentiary rules to provide criminal defendants with a substantive right to reliability testing through validation testing in cases involving AI. In the machine learning context, "validation" is defined "as the process where a trained model is evaluated with a testing

[243] *See* FED. R. EVID. 702, 901.
[244] *See supra* Section III.B.

data set."[245] Validation testing provides a "a [more accurate] estimation of the true risk of the output predictor of a learning algorithm."[246] Validation testing is, in some ways, analogous to the testing of a human witness's reliability through cross-examination. Just as a witness is tested for bias, lack of truthfulness, and for inconsistencies, an algorithm can be tested for accuracy through validation. Even if this comparison is a conceptual stretch, a right to validation testing of an AI system is likely more valuable than any right to cross-examine a human witness who may have limited insight into the parameters of the model's capabilities. Validation testing will directly target the model's reliability rather than rely on the technical knowledge of a human witness.

A full exploration of this proposal is beyond the scope of this paper. But there are many ways this right could be incorporated into the law of evidence. The right could be housed in amended provisions of the federal rules, derived from a reinterpretation of the Confrontation Clause, or judicially implied through a reinterpretation of Rule 901(b)(9) or *Daubert*. To be sure, the limits to this proposal are beyond merely finding a handhold for the right in existing law. One critical question is who exactly should finance this right to validation testing.[247] Trial courts could cover the costs; however, there are clear administrability objections to such a proposal. Shifting costs to the prosecution is certainly an option; but this may run the risk of indirectly discouraging the use of AI in criminal fact-finding.[248] In any case, placing the burden on the prosecution to front the costs may make the most sense; this is the party affirmatively choosing to use these systems to prosecute defendants.

CONCLUSION

AI in the courtroom poses unique problems for the law of evidence. This Paper has addressed only one aspect of this ongoing study of the intersection between AI and the law—criminal defendants' rights to confrontation under the Sixth Amendment. In a future where AI becomes more prevalent in its application to forensic sciences, criminal

[245] Haiying Wang & Huiru Zheng, *Model Validation, Machine Learning*, *in* ENCYCLOPEDIA OF SYSTEMS BIOLOGY 1406–07 (Werner Dubitzky et al. eds., 2013).

[246] Shai Shalev-Shwartz & Shai Ben-David, *Model Selection and Validation*, *in* UNDERSTANDING MACHINE LEARNING: FROM THEORY TO ALGORITHMS 116 (2014); Grzenda et al., *supra* note 64, at 726 (noting that "[e]xternal validation of trained models is essential to estimating the reproducibility of the model's behavior in real-world conditions but is rarely done").

[247] It is worth noting that indigent defendants may not be able to afford validation testing.

[248] This, in turn, may discourage future development of AI in the forensic context.

defendants' rights to confrontation will continue to erode. The precise practical effects of this erosion are difficult to measure, but there is good reason to believe that these limitations will negatively impact defendants' abilities to test the reliability of inculpatory AI-generated evidence. Notwithstanding the practical effects of this erosion, the diminishment of the right to confrontation is notable. In a world of cutting-edge science, the right to confrontation loses much of its utility and, potentially, its relevance. As scholars and jurists tackle the novel evidentiary issues at the junction of AI and the law, some attention should be given to the proper place of the right to confrontation under the Confrontation Clause. Without further reconsideration, this constitutional right may retreat into the background.